UNIVERSIDADE DE LISBOA
Faculdade de Ciências
Departamento de Informática

ANÁLISE DE RISCO ASSOCIADO A QUEBRAS DE SERVIÇO

Ricardo André Pereira Oliveira

Trabalho orientado pela Prof. Doutora Ana Luísa do Carmo Correia Respício

DISSERTAÇÃO

(Versão pública)

MESTRADO EM SEGURANÇA INFORMÁTICA

2015

Agradecimentos

Durante o desenvolvimento deste trabalho, muitas foram as sugestões de colegas de trabalho e amigos. Cabe-me aqui deixar expresso o meu reconhecimento a todos aqueles que, directa ou indirectamente, contribuíram para a realização deste trabalho.

A todos os meus Professores que sempre me deram uma mensagem de incentivo nos momentos difíceis e que assim me ajudaram a chegar até aqui.

À Professora Doutora Ana Respício, minha orientadora, dirijo um agradecimento muito especial pelo apoio, orientação, colaboração, amizade e disponibilidade, não devendo ainda ficar esquecida a oportunidade que me deu de realizar este trabalho.

Finalmente à minha família, pela paciência e pelo apoio que me deu durante a realização de todo o curso.

À minha filha Catarina

Resumo

O conceito de "risco" tem-se tornado cada vez mais presente na vida das organizações. Desde sempre que o Gestor de topo tem presente na sua consciência que gerir a vida da sua organização ou do seu sistema implica também a gestão do risco. Nos dias de hoje, o risco é universalmente entendido como um conceito que incorpora uma parte negativa que pode impedir as organizações de atingirem os seus objectivos mas também uma parte positiva que é a oportunidade de estas obterem ganhos.

Este documento descreve um trabalho autónomo que aborda um problema concreto a que uma determinada instituição bancária pretende dar resposta. Este problema prende-se com a necessidade de, por um lado, melhorar a estimativa de risco associado a possíveis quebras de serviço que possam ocorrer no futuro e, por outro, quantificar perdas associadas a quebras de serviço ocorridas no passado.

Este trabalho teve como objectivo valorar as perdas que uma determinada organização pode sofrer em consequência de um funcionamento deficiente, ou mesmo indisponibilidade, dos serviços que oferece aos seus clientes. Este mau funcionamento pode resultar de ataques bem-sucedidos à sua infra-estrutura informática ou de outros eventos que provoquem quebras de serviço.

Foi feito um levantamento das interacções entre os vários subsistemas e dos vários eventos que podem conduzir a estados de operação irregular, de forma a estabelecer relações de causalidade entre eles. Por outro lado, foi feita uma análise do histórico de eventos e suas repercussões de forma a estimar custos. Foi desenvolvida uma aplicação para auxiliar o processo de análise de risco associado à falha da infra-estrutura. Esta aplicação permite efectuar a modelação de sistemas, recolher métricas indicadoras do valor e desempenho dos processos que lhes estão associados e, com base nesta informação, estimar riscos relacionados com potenciais falhas, assim como, apurar perdas associadas a quebras de serviço efectivamente ocorridas. Procedeu-se à avaliação da utilidade e usabilidade da aplicação junto de decisores de alto nível de gestão que serão os seus futuros utilizadores na referida instituição.

Palavras-chave: Quantificação de Risco, Análise de Risco, Quebra de serviços, Disrupção, Falha, Valoração de falhas, Fiabilidade.

Abstract

The concept of "risk" has become increasingly present in the life of organizations. Senior managers have always had the notion that the effective organizational life has to deal with risk. Nowadays risk is universally known as a concept that incorporates both positive and negative aspects. The negative aspect of risk is what prevents the organization of achieving its goal while the positive are opportunities that can be explored to achieve more earnings.

This document describes an autonomous work addressing a concrete problem that a certain bank aims to deal with. This problem is related to the need of improving the estimation of risk associated with service failures that may occur in the future as well as quantifying losses due to service failures occurred in the past.

The current work aimed to assess the losses of value that an organization may suffer as a result of a malfunction or even unavailability of the services it offers to its customers. This malfunction can result from successful attacks on their IT infrastructure or other events that cause service breaks.

A survey was taken on the interactions between the several subsystems and the various events that can lead to irregular operating states, in order to establish causal relationships between them. An analysis of historical events and their effects was made in order to estimate costs.

An application was developed to assist the risk analysis process associated with infrastructure failure. It allows to model systems and collect metrics about the value and performance of processes associated with these systems. Based on this information, it is possible to estimate risk related with potential failures as well as determining losses from a failure that has occurred in the past.

The application was then evaluated for its utility and usability by senior managers to be used by the above organization.

Keywords: Quantification of risk, Risk analysis, Break of services, Disruption, Fault, Failures valuation, Reliability.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

"Existem dois tipos de risco: Aqueles que não nos podemos dar ao luxo de correr e aqueles que não nos podemos dar ao luxo de não correr." (Peter Drucker)

A gestão de risco é hoje genericamente aceite pela gestão de topo como uma actividade essencial à gestão como um todo, na prossecução dos objectivos de uma organização e no aproveitamento de oportunidades de crescimento e desenvolvimento. Trata-se de um processo contínuo de identificação, análise e controlo de factores de risco de forma proactiva e o seu objectivo é reduzir não só a probabilidade de um evento impactante de forma negativa ocorrer, mas também a magnitude do seu impacto.

Os sistemas de gestão de risco são projectados para fazer mais do que apenas identificar o risco. O sistema também tem de quantificar o risco e prever o seu impacto sobre a organização. O resultado deste processo consiste num risco residual que pode ser considerado aceitável ou inaceitável, dependendo do nível de tolerância definido pela organização.

Esta dissertação centra-se numa componente do processo de gestão de risco - a análise de risco - pretendendo ser um contributo para se conseguir afectar positivamente a qualidade deste processo. Pretende-se fornecer uma abordagem capaz de auxiliar a realização quer de estimativas, quer de apuramento do impacto de uma quebra de serviço ocorrida no passado, de forma a poder alcançar resultados com margens de erro reduzidas.

Neste primeiro capítulo apresenta-se a motivação para este tema, os objectivos que se pretenderam atingir com este trabalho, bem como os principais contributos que este vem oferecer. Apresenta-se ainda o plano de trabalho e considerações sobre este e, por fim, uma breve descrição da organização deste documento.

1.1 Motivação

O conceito de "risco" tem-se tornado cada vez mais presente na vida das organizações. Desde sempre que a gestão das organizações inclui também a gestão do risco. A gestão de risco dos seus investimentos, a gestão do risco inerente ao seu tipo de negócio, a gestão de risco de falhas no seu sistema, enfim, esta gestão está presente em todas as acções da vida de uma organização.

A crescente dependência das organizações em relação aos sistemas de informação, provoca a inclusão das questões relacionadas com a segurança e análise de risco destes nas decisões estratégicas e de gestão.

Por outro lado, a globalização do mercado, a busca incessante por uma gestão cada vez mais rentável dos recursos das organizações, em que as alianças estratégicas são cada vez mais frequentes, provocam constantes mutações no ambiente empresarial e necessariamente mutações ao nível do risco. Porém a gestão de risco é feita na maioria dos casos de forma empírica e não de uma forma planeada, sistematizada e quantificada.

Existe assim a necessidade de metodologias e ferramentas [1] que permitam modelar um sistema, equacionar pontos de falha, calcular probabilidades de falha, estimar ou constatar perdas com elevado grau de precisão e relacioná-las com determinada ocorrência.

No caso de alguns sectores de actividade, como por exemplo a banca, para além do facto das instituições se verem a braços com sistemas difíceis de monitorizar pela sua complexidade, os custos intangíveis como a perda de qualidade e reputação assumem grande importância podendo ter grande impacto na continuidade do negócio. Por outro lado, a gestão de topo tem grande dificuldade em arriscar a tomada de decisões baseadas em dados qualitativos, uma vez que estes lhes podem transmitir elevado gau de incerteza e ambiguidade [2]. A quantificação deste tipo de custos é um caminho ainda pouco explorado, pretendendo este trabalho ser também um contributo para lidar com este problema.

Uma vez que os recursos, humanos e materiais, são sempre escassos para qualquer organização face às necessidades de segurança de um sistema, é difícil para um Administrador conseguir efectuar esforços para garantir a segurança em todo o sistema. Assim a prioritização e o direccionamento de esforços constituem também uma necessidade premente.

No decorrer do trabalho que tenho vindo a realizar na instituição bancária a que pertenço, foram surgindo situações que se enquadram naquilo que acima foi descrito - a necessidade de assumir trabalhar com risco, gerir risco, mitigar risco. Por outro lado,

foram surgindo reorganizações e terciarização de recursos e serviços, levando a novas arquitecturas, novos riscos, novas necessidades de monitorização e imposição de SLA's (Service Level Agreement) a fornecedores. O panorama económico-social vivido no sector bancário nos últimos tempos leva também a que se enfrentem novos desafios no crescimento e salvaguarda da marca e da reputação da instituição [3]. É fundamental para os gestores encontrarem meios de medir de que forma, falhas nos seus sistemas e processos afectam estas variáveis.

A metodologia e ferramenta que este trabalho propõe pretendem contribuir para a resposta a estes problemas, auxiliando através da monitorização, ao direccionamento de esforços para os pontos do sistema que devem merecer mais atenção, evidenciando a probabilidade de falha e o impacto que cada processo representa em caso desta ocorrer. O resultado deste trabalho pretende também constituir uma ferramenta de apoio à decisão permitindo testar variações no nível de risco decorrentes de possíveis alterações que se possam efectuar na configuração dos sistemas analisados.

O sistema sobre o qual incidiu o trabalho foi o sistema Multibanco por representar um dos sistemas mais importantes da instituição, quer pelo volume de transacções que representa, quer pelo impacto que a sua componente de tempo-real provoca na qualidade do serviço e consequente reflexo no nível de satisfação do cliente final.

1.2 Objectivos

O principal objectivo desta dissertação foi, através da sistematização das tarefas inerentes ao processo de análise de risco, propor uma metodologia de quantificação e valoração de riscos associados a quebras de serviço, capaz de cumprir duas funções. Por um lado estimar o risco de um sistema num hipotético cenário de falha, por outro, valorar perdas relacionadas com uma quebra de serviço efectivamente ocorrida.

Foi também objectivo deste trabalho, o desenvolvimento de uma aplicação informática que, apoiada nesta metodologia, permitisse representar um sistema através da caracterização dos processos que o compõem e do estabelecimento de relações de dependência entre eles. A aplicação deveria permitir também a recolha ou importação de informação inerente ao sistema analisado de forma a poder cumprir as duas valências da referida metodologia.

Por fim, pretendia-se que esta aplicação e respectiva metodologia de apoio fossem validadas através de uma prova de conceito, realizada pelos utilizadores da instituição bancária a que se destina. A análise incidia sobre um sistema bancário, mais concretamente o Sistema Multibanco.

Apesar de todo o trabalho ter sido realizado com a preocupação de se adaptar ao sistema acima referido, sistema este que possui características de *workflow*, foi também desenhado com intuito de ser aplicável de forma genérica a outros sistemas com estas características.

1.3 Contribuições

A aplicação informática desenvolvida constitui, em conjunto com a metodologia proposta, uma ferramenta para sistematizar e facilitar o processo de análise de risco em sistemas que possam ser modelados através de um *workflow*. Assim, considera-se que as principais contribuições desta dissertação são:

- **A elaboração de uma metodologia de quantificação e valoração de risco**: metodologia que funcionando baseada em recolha e tratamento de informação, permite o registo de métricas inerentes aos processos que compõem um determinado sistema. Essas métricas permitem calcular o valor dos processos que relacionado com outros factores inerentes ao cálculo de risco, nomeadamente a probabilidade de falha, o grau de mitigação, entre outros, permitem apurar o valor do risco do sistema. Por outro lado, a comparação dessas métricas ao longo do tempo permite estabelecer uma relação de causalidade entre uma quebra de serviço efectivamente ocorrida e determinado padrão observado nas métricas recolhidas, tornando assim possível valorar a eventual perda associada. Considerando a importância da componente de análise de risco para o sucesso do processo de gestão de risco como um todo, a metodologia proposta procura sistematizar as tarefas a ela inerentes, de forma a facilitar e melhorar a análise de risco em sistemas com grande grau de complexidade. Esta metodologia sugere inclusive formas de quantificar riscos tidos como intangíveis como é o caso da reputação.
- **Uma ferramenta de apoio à decisão**: a aplicação desenvolvida, ao permitir uma análise quantitativa de risco, contribui para a diminuição da subjectividade, ambiguidade e incerteza nas decisões que a gestão de topo tem de tomar face ao risco, possibilitando tomar essas decisões de uma forma mais informada e baseadas numa análise *custo-benefício*. O apoio à decisão é fornecido pelas seguintes funcionalidades:
    - **Representação de sistemas**: tratando-se a aplicação informática produzida ao longo deste trabalho de uma implementação da metodologia desenvolvida, o seu funcionamento acaba por estar assente na caracterização dos vários processos que compõe um sistema. O utilizador pode utilizar esta ferramenta para saber que processos

compõem determinado sistema, quais as dependências entre eles, quais os vários sistemas de que fazem parte, quais os activos e variáveis lhe estão associados e respectivo valor. A aplicação é também capaz de indicar quais os processos mais críticos, permitindo assim direccionar a atenção do responsável do sistema. Uma vez que os sistemas analisados são representáveis em *workflow*, o utilizador tem a possibilidade de visualizar uma representação de um determinado sistema inserido na aplicação, através de um diagrama BPMN gerado automaticamente a partir desta.

- **Estimativa de risco**: a aplicação desenvolvida proporciona um meio de estimar o impacto de uma falha futura em qualquer processo do sistema, por concretização de uma determinada ameaça. Esta estimativa pode ter por base informação acerca dos processos obtida de forma empírica ou informação de histórico do sistema em análise, proporcionando previsões mais sustentadas.
- **Avaliação de diferentes configurações de um sistema:** a aplicação possibilita ainda a modelação de configurações diferentes de um determinado sistema em análise, de forma permitir a comparação, numa base quantitativa, entre os níveis de risco daí resultantes.
- **Análise do impacto de falhas:** uma outra valência desta aplicação é a possibilidade de quantificar perdas decorrentes de uma quebra de serviço ocorrida no passado, efectuando comparações de padrões de comportamento de um determinado sistema, entre o período de falha e períodos homólogos, através da utilização de informação de histórico desse mesmo sistema em análise.
- **Definição de SLA**: quando uma organização procede à terciarização de serviços e respectivos sistemas a eles afectos, torna-se importante a definição dos SLA perante os seus fornecedores. Esta ferramenta pode auxiliar nessa tarefa, uma vez que fornece uma visão da evolução temporal do impacto das quebras de serviço.

1.4 Planeamento

Apresentam-se na Tabela 1 as principais deadlines do projecto e respectivos produtos entregues.

Relativamente ao plano inicial verificaram-se atrasos em algumas tarefas. A tarefa "Elaboração do documento de especificação da aplicação informática a desenvolver" sofreu um atraso de duas semanas no seu arranque motivado por eu ter sofrido de

doença temporariamente incapacitante. Este atraso reflectiu-se na data de início de todas as tarefas subsequentes.

Adicionalmente a tarefa "Elaboração do Relatório Final" sofreu um atraso de aproximadamente um mês motivado por dificuldades de conciliação de agenda entre mim e os utilizadores finais deste trabalho e entre mim e a orientadora da dissertação durante o mês de Agosto. Para este último facto também pesou significativamente o facto de eu ser trabalhador estudante.

Tabela 1 - Planeamento previsto no relatório preliminar

Período	Tarefas	Entregáveis
15/10/2014 a 30/11/2014	Análise de documentação e trabalhos relacionados; Análise do Sistema a utilizar como prova de conceito.	Relatório Preliminar
01/12/2014 a 31/12/2014	Conclusão da definição do método de Análise de risco.	
01/01/2015 a 31/01/2015	Elaboração do documento de especificação da aplicação informática a desenvolver.	
01/02/2015 a 14/05/2015	Desenvolvimento da Aplicação Informática.	Aplicação Informática
15/05/2015 a 14/06/2015	Testes de utilização da ferramenta.	Relatório de testes
15/06/2015 a 15/07/2015	Elaboração do Relatório Final.	Relatório Final

1.5 Estrutura do documento

Este documento está organizado da seguinte forma:

Capítulo 2 – Análise e gestão de risco em Segurança informática: Neste capítulo são apresentados alguns conceitos fundamentais relacionados com o tema deste trabalho, de forma a permitir a sua contextualização e o seu posicionamento dentro do processo de gestão de risco. São também descritas as principais normas relacionadas com a gestão de risco em segurança da informação e apresentados alguns trabalhos e ferramentas existentes que estão de alguma forma relacionados com o problema a que este trabalho pretende responder, tendo servido de inspiração ou apoio para o desenvolvimento deste projecto.

Capítulo 3 – Metodologia para quantificação de risco no sistema Multibanco: Este capítulo contém a descrição do sistema usado na prova de conceito, da metodologia de quantificação e valoração de risco proposta e da forma como esta foi aplicada ao sistema.

Capítulo 4 – Quanto – Aplicação de quantificação de risco: Este capítulo apresenta a especificação da aplicação de quantificação de risco desenvolvida. Começa por apresentar a especificação de requisitos, a sua arquitectura, as ferramentas utilizadas e por fim as funcionalidades que compõem a aplicação.

Capítulo 5 – Avaliação da Ferramenta Quanto: Este capítulo contém a avaliação efectuada ao trabalho realizado decorrente da utilização pelos seus futuros utilizadores. Nele estão descritos os principais enfoques dos testes de utilização e as conclusões daí retiradas.

Capítulo 6 – Conclusão: Neste capítulo são apresentadas as considerações finais sobre a dissertação, fazendo uma revisão dos objectivos, propostas para trabalho futuro e conclusões finais.

Capítulo 2

Análise e gestão de risco em Segurança Informática

Neste capítulo apresentam-se alguns conceitos fundamentais ligados ao tema deste trabalho e que permitem contextualizar o seu posicionamento dentro do processo de gestão de risco. Começa-se por apresentar as noções de "Risco", "Gestão de risco" e "Apreciação de risco", passando também pela descrição das principais normas ISO existentes sobre este tema.

Apresentam-se ainda algumas das metodologias de avaliação de risco mais conhecidas e uma breve descrição sobre a pesquisa efectuada por trabalho relacionado com o tema, dando-se especial destaque aos trabalhos sobre o impacto das falhas na confiança dos clientes, métodos de cálculo de fiabilidade em sistemas de *workflow* e trabalhos sobre a importância dos SLA.

2.1 Risco

Falar sobre o processo de gestão de risco obriga em primeiro lugar a falar da definição de risco.

A noção geral do conceito de risco foi evoluindo ao longo do tempo. No passado este conceito tinha apenas uma conotação negativa ligada ao perigo e à perda e por isso qualquer acção estratégica em que fossem identificados riscos, simplesmente era de evitar. Mais tarde as organizações foram entendendo o risco como algo inerente à sua actividade e à oportunidade de alcançar objectivos e que por isso devia ser gerido como outro recurso qualquer.

A norma NP ISO 31000:2013 define risco de uma forma extremamente abrangente e generalista: "Efeito da incerteza na consecução dos objectivos. Um efeito é um desvio, positivo ou negativo, relativamente ao esperado. Os objectivos podem ter diferentes

aspectos (financeiros, de saúde e segurança, ambientais, entre outros) e podem ser aplicados a diferentes níveis (estratégico, em toda a organização, de projecto, de produto e de processo). O risco é frequentemente caracterizado pela referência aos eventos potenciais e consequências, ou à combinação de ambos. A incerteza é o estado, ainda que parcial, de deficiência de informação relacionado com a compreensão ou conhecimento de um evento, sua consequência ou probabilidade" [4].

No contexto específico de segurança da informação, risco é a possibilidade de uma ameaça explorar vulnerabilidades de um activo ou conjunto de activos, do qual pode resultar prejuízo num sistema. É medido em termos de combinação da probabilidade de um evento negativo ocorrer (ex. uma ameaça conseguir explorar uma vulnerabilidade) e as perdas ou prejuízos causados num activo ou conjunto de activos - ISO/IEC 13335-1 [5].

Whitman et al. [6] apresenta as principais métricas utilizadas para cálculo de risco. As componentes básicas para calcular risco são o valor do activo e a probabilidade de uma falha acontecer. Estas duas componentes permitem-nos calcular aquilo que se designa por "risco base", de acordo com a seguinte fórmula:

Risco base=Valor do Activo * Probabilidade de falha

Para estimar o valor do risco importa também ter conta a percentagem de risco que possa ter sido mitigada e também o grau de incerteza face à probabilidade de falha e grau de mitigação afirmados. Surge assim o conceito de "risco relativo" que pode ser calculado utilizando a seguinte fórmula:

Risco relativo=Risco base – (Riso base * % incerteza) - (Risco base * % mitigação)

A tomada de medidas de controlo de risco acarreta custos na maioria dos casos. A tomada dessa decisão é usualmente sustentada por uma análise custo-benefício feita para apurar a exequibilidade de determinada medida, opondo o custo de um controlo contra o benefício potencial desse controlo. Em termos de segurança da informação, esse benefício é expresso pela diminuição no valor anual de perda inerente a determinado activo de informação. Este valor é designado por ALE (Annualized Loss Expectancy) e é calculado pela seguinte fórmula:

ALE=SLE * ARO

Nesta fórmula SLE (Single Loss Expectancy) representa a estimativa de dano por cada ameaça e ARO (Annualized rate of Occurrence) representa o número anual estimado de ocorrências [7]. O valor do ALE pode depois ser comparado com o custo de determinada solução e com o valor de mitigação que se espera obter com a sua implementação.

2.2 Gestão de risco

A norma portuguesa ISO 31000:2013, de forma muito sintética, define o processo de gestão de risco como “Actividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco” [4].

De acordo com a Agência Europeia para a Segurança das Redes e da Informação (ENISA), gestão de risco é "um processo que visa um equilíbrio eficiente entre perceber as oportunidades de obter ganhos e minimizar as vulnerabilidades e as perdas" [8]. Além disso, é uma parte integrante das práticas de gestão e crucial para alcançar uma boa governança corporativa.

A NP ISO 31000:2013 apresenta a organização do processo de gestão de risco conforme ilustrado na Figura 1. Aqui é visível que o processo de gestão de risco deve ser um processo cíclico. No entanto, as componentes de “Monitorização e revisão” e “Comunicação e consulta” não acontecem de forma estanque no processo global de gestão de risco. Em vez disso, estas actividades são contínuas, funcionando em paralelo com todas as outras actividades, recolhendo e fornecendo informação a estas.

Para além de atribuir esta importância à comunicação e consulta, a NP ISO 31000:2013 considera também uma actividade de estabelecimento do contexto. Nesta actividade, a organização enuncia os seus objectivos, define os parâmentros internos e externos a ter em consideração quando se gere o risco. Por outro lado, a organização define também o âmbito e os critérios do risco para as restantes partes do processo.

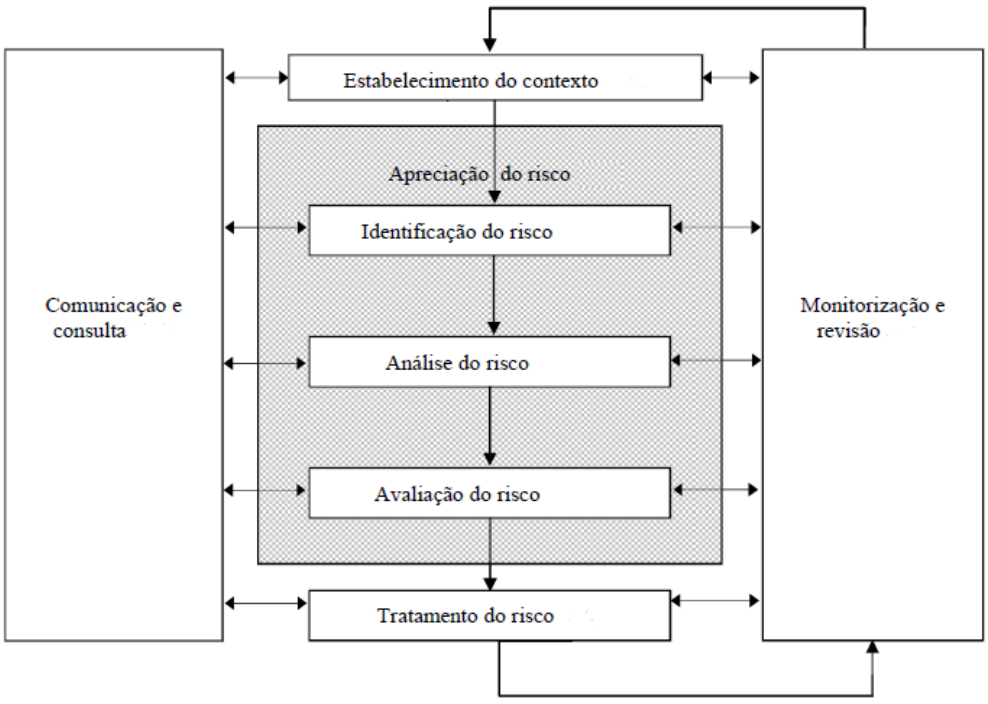

Figura 1 - Processo de gestão de risco – NP ISO 31000:2013

Rausand [9] apresenta uma visão do processo de gestão de risco em quase tudo alinhada com a norma ISO referida. Na Figura 2 podemos ver a sua representação do processo e as diversas actividades inerentes a cada componente. Tais actividades tipicamente incluem, ao nível da análise de risco, a identificação de ameaças para determinados activos, probabilidades de falha e nível de risco. A componente da avaliação de risco compreende a análise e prioritização dos riscos, avaliação do nível de risco tendo em conta os critérios de aceitação de risco previamente definidos e a proposta de medidas de controlo de risco. Na componente de controlo tem lugar a aplicação de medidas de tratamento de risco e respectivo acompanhamento dos resultados. Nesta última componente existe uma ligeira diferença face à NP ISO 31000, uma vez que o autor considera que nela estão incluídas as actividades de tratamento de risco.

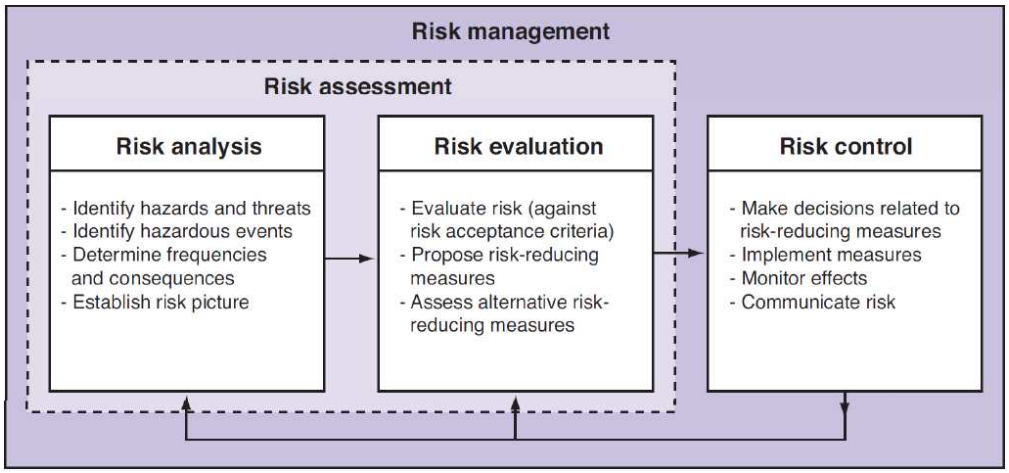

Figura 2 - Actividades do processo de gestão de risco – Rausand [9]

Apesar da diferença existente na fase de controlo, todas as actividades também consideradas pela norma ISO 31000 estão presentes no modelo. Conforme representado na Figura 3, trata-se também de um processo que deve ser contínuo ou cíclico onde a componente da comunicação tem importância transversal a todo o processo e que tem como orientação conseguir uma aplicação coordenada e eficiente dos recursos de forma a minimizar, monitorar e controlar a probabilidade e/ou impacto de eventos negativos.

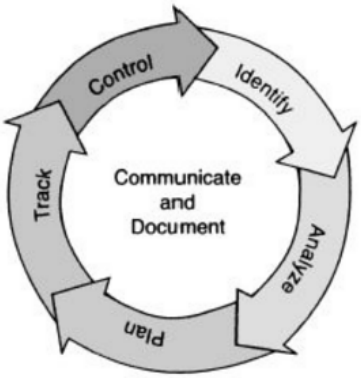

Figura 3 - Visão cíclica do processo de gestão de risco – Rausand [9]

2.3 Apreciação de risco

Uma etapa fundamental no processo de gestão de risco de segurança da informação é a apreciação de risco (*risk assessment*). Esta envolve a análise de cada risco, bem como a análise do total de riscos dando-lhes prioridades relativas. Apesar de esta actividade existir como parte do processo de gestão de risco, ela não é contínua mas sim uma actividade distinta, sendo apenas iniciada quando necessário ou em intervalos regulares.

A apreciação de risco serve para identificar e analisar possíveis vulnerabilidades e ameaças para um dado sistema, bem como o valor relativo dos seus bens e possíveis danos resultantes do seu comprometimento. Esta actividade é feita com o objectivo de estimar o risco de que o proprietário, o operador ou o utilizador do sistema pode enfrentar. Como tal, o seu resultado é a base para as restantes actividades de gestão de risco, permitindo desencadear o tratamento do risco de onde podem surgir novos requisitos de segurança, a escolha e especificação de contramedidas, necessidade de avaliação das políticas de segurança actuais e avaliação dos mecanismos de protecção e controlo existentes. Tudo isto poderá servir para apoiar decisões de gestão relevantes.

O principal resultado de uma apreciação de risco é geralmente uma avaliação qualitativa ou quantitativa dos possíveis riscos a que um determinado sistema complexo está exposto, levando em consideração o seu contexto e as ameaças prováveis. Deve-se salientar que a maioria das apreciações de risco, bem como a maioria dos processos de gestão de risco implementados, não visam a obtenção de um sistema totalmente seguro, até porque na maioria das vezes isso seria impossível. Em vez disso, o objectivo final é chegar aquilo que possa ser entendido como o nível de segurança aceitável a um custo aceitável. As diversas *frameworks* existentes neste contexto diferem na interpretação que fazem deste processo e no modo de como o conseguir e manter.

Na Figura 1 da secção 2.2, também se pode observar como é entendido, de uma forma geral, o subprocesso de apreciação de risco. Alguns trabalhos realizados sobre o tema consideram a actividade de "Estabelecimento do contexto" como fazendo parte do processo de apreciação do risco, outros, nem sequer consideram esta actividade como fazendo parte do processo de gestão de risco. No entanto é indiscutível que esta actividade é necessária à boa governação dos sistemas e à gestão do risco por inerência. Esta fase pode ser encarada como opcional, uma vez que pode já existir uma boa especificação do sistema feita no âmbito de outra actividade. Trata-se de identificar e definir o contexto técnico, social e de negócio em que o sistema opera, bem como a construção de algum tipo de modelo do próprio sistema de informação. Nesta fase

também se executam outras actividades relevantes como definir a escala de avaliação, os requisitos de segurança, objectivos de stakeholders, critérios de risco etc.

A apreciação do risco é uma tarefa multidisciplinar que envolve as seguintes fases:

- **Identificação de riscos**: este é o núcleo de qualquer análise de risco e, no caso da segurança de informação, consiste no uso de dados disponíveis para identificar possíveis vectores de ataque e vulnerabilidades do sistema. O objectivo desta etapa é gerar uma lista de eventos que sejam capazes de afectar de alguma maneira a consecução dos objectivos de um sistema ou organização. Apenas os riscos identificados serão alvo das análises a realizar nas etapas seguintes.
- **Análise dos riscos**: este passo tem a ver com a compreensão das probabilidades, apuramento de impactos e outros parâmetros associados aos riscos identificados, a fim de permitir uma melhor compreensão das vulnerabilidades do sistema. É nesta componente específica do processo que se insere o presente trabalho.
- **Avaliação dos riscos**: nesta etapa os riscos são classificados e prioritizados, a fim de permitir que os agentes de decisão possam decidir sobre contramedidas a tomar. A avaliação do risco envolve a comparação do nível de risco identificado na etapa de análise com os critérios de aceitação do risco definidos na fase de "Estabelecimento de contexto". Esta comparação pode ou não indicar uma necessidade de tratamento de risco. Embora o passo de selecção de contramedidas seja muitas vezes considerado como fora do âmbito de uma avaliação de risco, é comum que os resultados obtidos com os passos acima possam ser usados de alguma forma para a selecção ou prioritização de contramedidas, estratégias de mitigação, controlos de segurança ou políticas de segurança, a serem implementados na fase de "Tratamento do risco".

2.4 Normas ISO

A problemática da Segurança da Informação está associada com a crescente dependência das empresas dos Sistemas de Informação e Tecnologias da Informação. Reconhecendo o valor da informação, as organizações devem certificar-se de que a gerem de forma eficaz.

Um Sistema de Gestão de Segurança da Informação (SGSI) deve permitir uma eficiente gestão dos riscos de segurança da informação e deve por isso assumir grande importância estratégica nas decisões das organizações.

No contexto em que este trabalho foi desenvolvido, é importante realçar a importância de algumas normas que consubstanciam a necessidade de gerir o risco em segurança da informação, bem como, estabelecem conceitos e directrizes para a criação de mecanismos neste âmbito.

Nesta secção são apresentadas essas normas, descrevendo os seus objectivos e aplicação e apresentando as vantagens de conciliação destas.

2.4.1 NP ISO 31000:2013

A norma NP ISO 31000:2013 aplica-se a qualquer tipo de organização e estabelece um conjunto de princípios que deverão ser cumpridos de modo a tornar eficaz a gestão do risco. Recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objectivo é integrar um processo para gerir o risco na governação, estratégia e planeamento, gestão, processos de reporte, políticas, valores e cultura [4].

Desta norma é emanada uma série de termos e conceitos que permitem a universalização do dicionário a usar no contexto da gestão de risco, sendo a estrutura conceptual mais actual e podendo ser considerada como o estado da arte em matéria de gestão de risco. Pode ser considerada como o principal pilar em que assenta esta dissertação.

Para além de esta norma definir o processo de gestão de risco, define também toda uma estrutura que é necessário assegurar por parte da organização para que a sua implementação, manutenção e melhoria contínua sejam possíveis.

Princípios da gestão de risco

Segundo esta norma, as organizações que persigam o objectivo de implementar uma gestão de risco eficaz, devem actuar segundo uma lista de princípios nela definidos. A seguir realçam-se aqueles que mais directamente se relacionam com os objectivos desta dissertação:

- **A gestão de risco deve criar e proteger valor.** A gestão de risco deve contribuir de forma evidente para o alcance dos objectivos das organizações, melhoria da qualidade dos seus produtos e serviços, bem como, para o aumento da eficiência dos mecanismos de protecção e preservação dos seus activos.
- **A gestão de risco deve ser parte da Tomada de Decisão**. A gestão de risco deve servir para apoiar os decisores fornecendo-lhes informação capaz de suportar as suas opções face ao risco.

- **A gestão de risco deve ser Sistemática e Estruturada**. A gestão de risco deve poder contar com meios capazes de sistematizarem o processo de forma a produzir resultados atempadamente e que sejam consistentes e comparáveis.
- **A gestão de risco deve ser baseada na melhor informação disponível**. O processo deve ser alimentado com informação proveniente de várias fontes como histórico dos sistemas, pareceres de especialistas, registo de eventos, entre outro, mas tendo sempre em conta a qualidade relativa dos dados.

Estrutura da gestão de risco

A estrutura da gestão de risco é constituída por um conjunto de elementos que deve fazer parte do conjunto de políticas estratégicas e operacionais das organizações e deve conduzir as suas práticas com o objectivo de garantir o sucesso da aplicação de um processo de gestão de risco e possibilitar a sua melhoria contínua. Estes elementos fornecem os fundamentos da gestão de risco que são a política, os objectivos, o mandato e o compromisso para a gestão de risco mas também fornecem as disposições organizacionais como os planos, a responsabilização, os recursos, processos e actividades que irão permitir a aplicação do processo.

A estrutura da gestão de risco tem de garantir que toda a informação sobre risco seja correctamente reportada de forma a servir de base à tomada de decisão. A Figura 4 mostra as componentes necessárias a uma estrutura de gestão de risco e a forma como estas se relacionam iterativamente.

A componente de "Mandato e compromisso" representa o envolvimento imprescindível da gestão de topo na definição e aprovação de políticas de gestão de risco, na difusão desta cultura por todas as áreas, na alocação de recursos e atribuição responsabilidades e no alinhamento dos objectivos da gestão de risco com a estratégia da organização.

A componente "Monitorização e revisão da estrutura" é responsável por assegurar continuamente que a estrutura responde de forma eficaz ao seu objectivo. O seu desempenho deve ser medido periodicamente assim como os desvios face ao plano. A informação resultante deste processo deve servir de suporte a decisões sobre alteração de políticas, planos e estruturas com vista à melhoria da gestão de risco.

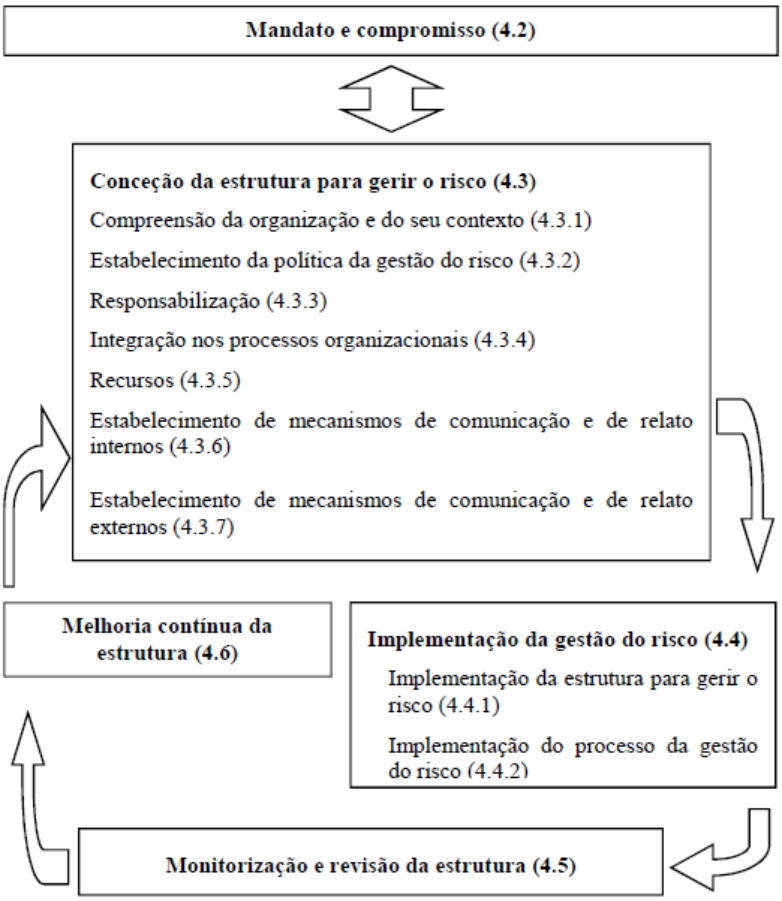

Figura 4 - Estrutura da gestão de risco - NP ISO 31000:2013

Processo de gestão de risco

O processo de gestão de risco deverá ser parte integrante da gestão, deverá fazer parte da cultura das organizações e deverá perceber o contexto em que estas se inserem de forma a poder ser feito à medida dos seus processos de negócio.

A Figura 1 apresentada na secção 2.2 ilustra o processo de gestão de risco delineando todas as suas componentes. Nela podemos ver que se destacam duas componentes por serem transversais a todo o processo. A "Comunicação e consulta" e a "Monitorização". Os planos iniciais devem considerar também os planos de comunicação e consulta de informação relacionada com o risco. Desta forma poder-se-á assegurar que todas as partes interessadas compreendem as razões que possam estar na base de decisões tomadas e porque são necessárias determinadas acções. A monitorização e revisão, por seu turno, irão permitir recolher métricas acerca de todas as fases do processo, podendo fornecer bases para a realização de ajustes e melhorias em todo o processo.

A actividade "Estabelecimento do contexto" levará em conta todas as questões internas ou externas à organização, relevantes para definição da finalidade do processo.

Nesta fase deverão ser feitas a definição de metas e objectivos das actividades de gestão de risco bem como a definição de responsabilidades e dos critérios de risco.

No processo de gestão de risco existe um sub-processo complexo designado por "Apreciação de risco" que compreende três actividades:

- **Identificação do risco**. Consiste em identificar as fontes de risco, áreas de impacto, eventos, respectivas causas e consequências.
- **Análise do risco**. Implica desenvolver uma compreensão do risco, quantifica-lo e até valora-lo, considerar as suas causas, consequências, probabilidade de ocorrência e factores capazes de influenciar estes. O seu *output* é o *input* para a avaliação de risco e é nesta fase que o trabalho desenvolvido nesta dissertação pretende ser um contributo.
- **Avaliação do risco**. A finalidade desta actividade é apoiar a tomada de decisões quanto à necessidade de os riscos serem tratados e à prioridade com que isso é feito.

A componente "Tratamento de risco" tem como input o resultado da actividade "Avaliação do risco" e implica a execução de duas tarefas, a selecção de opções de tratamento de risco e a preparação e implementação dos planos de tratamento de risco que basicamente documentam a selecção de opções efectuada. Esta actividade pode ser vista em maior detalhe na secção 2.4.4 sobre a norma ISO/IEC 27005.

2.4.2 ISO/IEC 27000

A norma ISO/IEC 27000 [10] contém uma visão geral e introdutória a toda a família ISO 27000.

A série de normas ISO 27000 constitui um padrão de certificação de sistemas de gestão, aplicado à implementação de um SGSI (Sistema de Gestão de Segurança de Informação), através do estabelecimento de uma política de segurança, de controlos adequados e da gestão de riscos. Esta família de normas, inclui padrões que definem os requisitos para um SGSI bem como para a sua certificação e prestam apoio directo e orientação detalhada para os processos e requisitos do ciclo PDCA (Plan, Do, Check, Act), adoptado como abordagem de processo para o SGSI.

A norma ISO 27000 em particular, serve de apoio a qualquer tipo de organização que pretenda entender os fundamentos, princípios e conceitos que permitem uma melhor gestão dos seus activos de informação. Tem como objectivo principal evitar diferentes interpretações de conceitos técnicos e de gestão e por isso contém termos e definições utilizados ao longo de toda a série 27000 sobre o ponto de vista da Tecnologia da Informação e das Técnicas e Gestão de Segurança. A norma define termos importantes

como por exemplo: Activos, Risco de Segurança da Informação, Gestão de risco, Análise de risco, Ameaça, Vulnerabilidade, entre outros.

Para além do estabelecimento do glossário e vocabulário, esta norma fundamenta a importância do SGSI para as organizações, definindo estratégias de como estabelecer, monitorar, implantar e melhorar, descrevendo os factores críticos de sucesso para a sua adopção nas organizações e apontando os benefícios de se usar uma abordagem padronizada para um SGSI. Os benefícios, para além do principal que é a diminuição do risco e/ou do seu impacto, passam também pela utilização de uma metodologia clara e universalmente aceite, com um processo de gestão assente numa *framework* estruturada que promove a utilização de boas práticas em segurança da informação, abrindo espaço para as especificidades inerentes à realidade de cada organização em particular, e pelo aumento da confiança dos stakeholders na organização.

Dado o seu caracter introdutório, a norma refere também como funciona o relacionamento entre as várias normas da família 27000.

2.4.3 NP ISO 27001:2013

A norma NP ISO 27001:2013 deriva da versão inglesa ISO/IEC 27001:2013 que por sua vez vem substituir uma primeira edição lançada em 2005. Foi preparada pela comissão técnica de Normalização CT 163 “Segurança em sistemas de informação”, cuja coordenação é feita pelo Organismo de Normalização Sectorial, itSMF Portugal (ONS/ITSMF).

A norma foi elaborada para especificar os requisitos para o estabelecimento, implementação, operacionalização, monitorização, revisão, manutenção e melhoria de um SGSI, dentro do contexto dos riscos de negócio de uma organização. Neste contexto estão envolvidas todas as actividades de gestão e as estruturas de suporte à gestão relevantes para a segurança da informação.

A implementação da norma 27001 pretende fazer com que as organizações mantenham o seu foco nas necessidades do negócio mas considerando a segurança da informação como parte integrante dos objectivos de negócio para realizar a gestão dos riscos.

A norma ISO 27001 é universal para todos os tipos de organizações, sejam elas comerciais, governamentais, com ou sem fins lucrativos, mas transmite flexibilidade na especificação dos requisitos para a implementação de controlos de segurança que podem ser personalizados consoante as necessidades de determinada organização.

Para além da interligação existente entre esta norma e outras da série 27000, existe um alinhamento explícito com a norma ISO 31000:2013 atrás descrita, o que pode ser constatado pela presença de referências à mesma, em várias das suas cláusulas.

As organizações que optam por obter a certificação nesta norma sujeitam-se a um processo de auditoria em duas fases. Numa primeira fase é feita uma revisão linear da documentação chave, bem como, da política de segurança da organização, declaração de aplicabilidade (SOA – Statement of Aplicability) e plano de tratamento de risco (PTR). Posteriormente é realizada uma auditoria em profundidade envolvendo o controlo do SGSI declarado no SOA e PTR, bem como a documentação de suporte. Preconizando a ideia subjacente a este conjunto de normas, a sua aplicação implica revisões periódicas confirmando que o SGSI mantém a sua aplicabilidade e operacionalidade.

A aplicação da norma ISO/IEC 27001 envolve o desenvolvimento de trabalho ao nível das seguintes componentes:

1. **Contexto da organização:** relativamente a esta componente a norma define que é necessário compreender a organização e o seu contexto assim como questões internas e externas relevantes para a sua finalidade e compreender as necessidades e expectativas das partes interessadas. Deve ser determinado o âmbito em que vai ser estabelecido o SGSI. Esta tarefa implica implementar e operar o sistema, monitorá-lo e analisá-lo criticamente de forma a poder melhorá-lo continuamente.
2. **Responsabilidades da liderança:** deve ser assegurado o comprometimento da liderança para com o SGSI e garantido que a política e objectivos de segurança da informação estão alinhados com a estratégia da organização. A liderança deverá efectuar a atribuição de responsabilidades e autoridades para as funções mais relevantes em termos de segurança da informação.
3. **Planeamento:** nesta componente a norma especifica que a organização deve proceder à identificação e endereçamento de riscos e oportunidades para o sistema de gestão e definir objectivos claros e critérios que possam ser usados para medir o seu sucesso. Deve definir um processo de avaliação de risco que considere os critérios de risco da organização e que inclua a identificação, análise e avaliação periódica dos riscos, identificando os responsáveis por estes. Deve ser também definido um processo de tratamento do risco, o que engloba seleccionar opções de tratamento de risco (reduzir, evitar, transferir, aceitar), determinar os controlos para as opções de tratamento escolhidas, produzir uma Declaração de Aplicabilidade baseada nos riscos/controlos identificados e elaborar um plano de tratamento do risco com a aprovação dos responsáveis pelos riscos.

4. **Suporte:** esta componente compreende vários aspectos que a organização deve assegurar e que conferem suporte ao sistema, nomeadamente, alocação de recursos e determinação de competências necessários ao funcionamento do SGSI, consciencialização de todas as pessoas da organização para as políticas de segurança, determinação de necessidades internas e externas de comunicação e documentação de toda a informação inerente ao processo.
5. **Desempenho do SGSI:** a organização deve periodicamente avaliar a eficácia do sistema. Previamente deve determinar o que deve ser monitorizado e quais os métodos a usar. Devem ser efectuadas auditorias internas para verificar se o SGSI responde aos requisitos da norma e aos requisitos de segurança identificados pela organização. A liderança da organização, com base no resultado das auditorias, deve efectuar uma análise crítica apontando oportunidades de melhoria do SGSI.
6. **Melhoria do SGSI:** corroborando o ponto 5, a melhoria contínua deverá ser conseguida através do uso da política estabelecida, resultados das auditorias, análise dos eventos monitorizados e acções correctivas de não conformidades encontradas.

2.4.4 ISO/IEC 27005:2008

A norma ISO 27005 estabelece directrizes para a gestão de risco em Segurança da Informação, fornecendo indicações para implementação, monitorização e melhoria contínua do sistema de controlos [11]. Esta norma refere conceitos, modelos e processos já descritos na norma ISO 27001 e pode ser usada para endereçar riscos específicos de TI. A norma 27005 é aplicada a todos os tipos de organizações que se destinam a gerir os riscos que possam comprometer a segurança da sua informação.

Esta norma divide-se nas seguintes componentes do processo de gestão de risco em segurança da informação:

- Estabelecimento do contexto
- Apreciação de risco
- Tratamento de risco
- Aceitação de risco
- Comunicação de risco
- Monitorização e revisão de risco

Todas as normas da série 27000, incluindo as duas citadas nos pontos anteriores, sugerem um modelo para que a implementação de um SGSI ocorra com sucesso e que está explicitamente alinhado com a norma ISO 27005. A Gestão da Segurança da Informação deve ser realizada tendo em conta algumas medidas de controlo sugeridas

por ambas as normas – o modelo de processo PDCA (Plan – Do – Check - Act) e o processo de análise/avaliação e tratamento de riscos [11].

Modelo PDCA (Plan – Do – Check - Act)

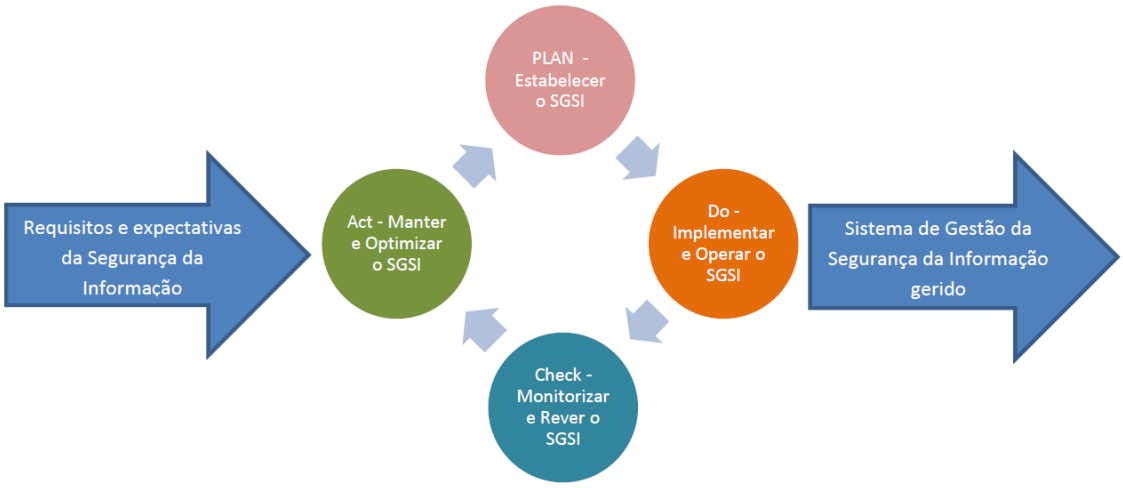

Figura 5 - Modelo PDCA

O modelo PDCA, representado na Figura 5, baseia-se no controlo dos processos e na verificação dos Sistemas de Segurança da Informação. O objectivo que a norma pretende obter com ele é a correcta gestão dos Sistemas de Segurança da Informação, tendo como base as expectativas e necessidades específicas de cada organização.

A Tabela 2 mostra um resumo das actividades do processo de gestão de risco em segurança da informação para cada uma das quatro fases do processo de gestão de segurança da informação, identificadas no modelo PDCA e que são executadas ciclicamente.

Tabela 2 – Alinhamento dos processos de gestão de segurança da informação e gestão de risco em segurança da informação

Processo de gestão de segurança da informação	**Processo de gestão de risco em segurança da informação**
Plan	– Estabelecimento do contexto – Apreciação de risco – Plano de Tratamento de risco – Aceitação de risco
Do	– Implementação do plano de tratamento de risco
Check	– Contínua monitorização e revisão dos riscos
Act	– Manutenção e melhoria do Processo de gestão de risco em segurança da informação

Apreciação de risco em segurança da informação

A Figura 6 apresenta o resumo do processo de apreciação de risco segundo a norma 27005, mais uma vez alinhado com a norma ISO 31000. No primeiro grupo podemos ver as actividades relacionadas com as componentes de identificação de riscos e no segundo grupo as actividades inerentes à análise e avaliação de risco o que corresponde ao subprocesso de apreciação de risco descrito na norma ISO 31000. Por fim o tratamento de risco formando o conjunto de actividades centrais do processo de gestão de risco.

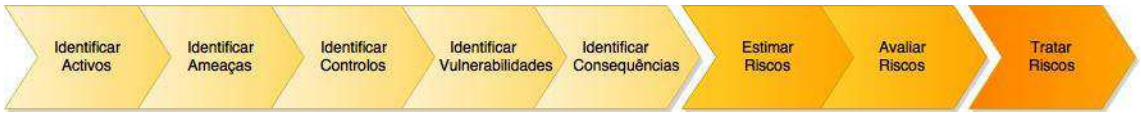

Figura 6 - Processo de apreciação de risco – ISO/IEC 27005:2008

Processo de tratamento de risco

A Figura 7 mostra o processo de tratamento de risco segundo a norma ISO 27005. Antes de se iniciar o processo de tratamento de risco, deverá ocorrer o processo de apreciação de risco, conforme já explicado em secções anteriores deste documento. Este processo termina na fase de avaliação de risco. Nesta altura deve ser avaliado se existe suficiente informação acerca do risco e se esta permite tomar decisões acerca das medidas a implementar de forma a manter o risco dentro dos níveis de aceitação de risco definidos pela organização. Se a resposta a esta avaliação for positiva, então termina o processo de apreciação de risco e pode-se iniciar o processo de tratamento de risco. Caso contrário, terá de ter lugar uma nova iteração de apreciação de risco com possível revisão do seu contexto e até redefinição de critérios de avaliação e aceitação de risco. Esta decisão corresponde ao ponto de decisão 1, visível na Figura 7.

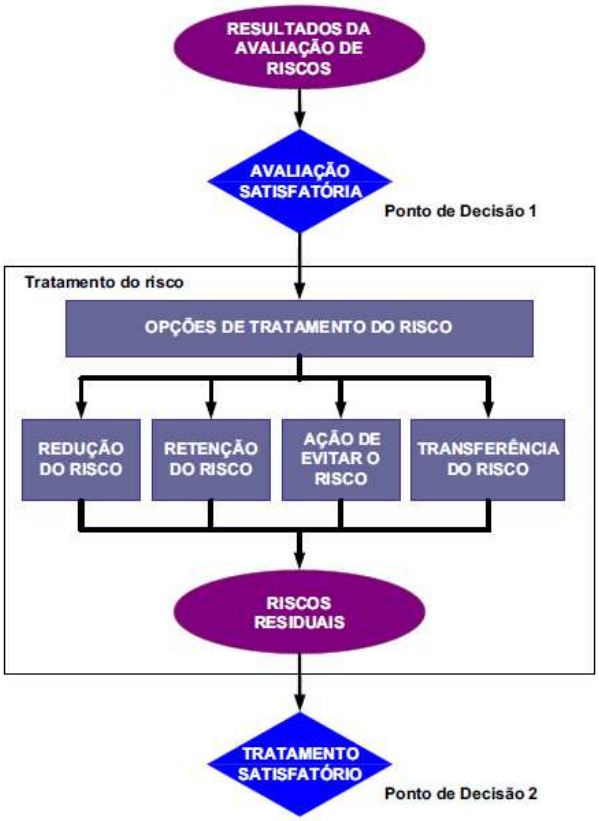

Figura 7 - Processo de tratamento de risco – ISO/IEC 27005:2008

As opções para tratamento do risco incluem quatro tipos de estratégia:

- **Reduzir o risco**. O nível de risco deve ser reduzido através da selecção de controlos até que o risco residual possa ser considerado aceitável. A acção pode passar por alterar a probabilidade das vulnerabilidades serem exploradas com sucesso, alterar o seu impacto ou até mesmo eliminar a fonte do risco;
- **Evitar o risco**. Identificar actividades ou condições que permitem que determinado risco possa ser evitado, podendo ser decidido parar ou não iniciar actividades;
- **Transferir o risco**. O risco deve ser transferido para outra(s) entidade(s) (exemplo: contractos com terceiros, financiamento de risco, seguros, etc.);
- **Aceitar o risco de forma informada**. Assumir o risco não efectuando nenhuma acção. Assumir o risco como condição para obter uma oportunidade.

Mais recentemente, propôs-se uma nova estratégia de tratamento de risco que corresponde a eliminar o activo que está ligado a determinado risco [6].

No ponto de decisão 2, acontece algo semelhante à primeira tomada de decisão. É possível que o resultado da primeira iteração de tratamento de risco não apresente um nível de risco residual dentro dos limites de aceitação de risco definidos pela organização. A eficácia do tratamento de risco depende da qualidade do processo de

apreciação de risco, pelo que, neste caso terá lugar nova iteração deste processo seguida de nova iteração do processo de tratamento de risco.

2.5 Metodologias de avaliação de risco

Nesta secção apresentam-se algumas das metodologias de avaliação de risco mais conhecidas. Das várias abordagens aqui descritas, independentemente de utilizarem escalas qualitativas ou quantitativas, todas convergem num ponto – é necessário conhecer o sistema em análise e recolher dele informação que permita estimar o impacto da ocorrência de uma falha. É precisamente nessa função que o produto resultante desta dissertação pretende dar resposta de uma forma quantitativa que permita ao decisor actuar com um grau de subjectividade tão pequeno quanto possível.

2.5.1 OCTAVE

A metodologia OCTAVE (Operaticonal Critical Threat, Asset and Vulnerability Evaluation), desenvolvida pela universidade Carnegie Mellon University, pretende operacionalizar alguns dos aspectos da gestão do risco, fornecendo uma abordagem para avaliar as necessidades de segurança da informação de uma organização [12]. O OCTAVE Allegro [13] é o método mais recentemente desenvolvido e baseia-se nas duas versões mais antigas designadas por OCTAVE e OCTAVE-S. O seu método é autodirigido, isto é, levado a cabo pelos próprios colaboradores das unidades de negócio alvo de análise e das unidades de TI que se organizam em pequenas equipas, contribuindo com o seu conhecimento e trabalhando em conjunto para responder às necessidades de segurança da organização. O método pode ser adaptado ao ambiente específico de cada organização em termos de risco, objectivos de segurança e capacidade. O OCTAVE direcciona uma organização para uma visão baseada em risco operacional de segurança aplicada num contexto de negócio.

O OCTAVE Allegro está vocacionado para activos de informação. Os activos importantes de uma organização são identificados e avaliados com base nos activos de informação a que estão associados. Este processo procura definir inequivocamente o âmbito de análise e reduzir a possibilidade de recolhas de dados demasiado extensas e consequentes análises desajustadas.

Esta metodologia pode ser realizada em *workshops* de ambiente colaborativo e é adequada para aquelas organizações que querem realizar a avaliação de risco sem um envolvimento organizacional extensivo.

O OCTAVE Allegro consiste em oito etapas organizadas em quatro fases:

1. Desenvolver critérios de medição de risco ajustados à missão da organização, aos seus objectivos e factores críticos de sucesso.
2. Criar um perfil de cada activo de informação crítico, estabelecendo de forma clara os seus limites, identificando os seus requisitos de segurança e identificando todos os seus repositórios.
3. Identificar as ameaças para cada activo de informação no contexto dos seus repositórios.
4. Identificar e analisar os riscos para activos de informação e começar a desenvolver abordagens de mitigação.

Apesar deste novo módulo da metodologia OCTAVE possuir uma visão mais orientada aos processos e serviços suportados por determinado activo de informação, não deixa de ser apenas um guia para garantir que os principais passos serão efectuados no que respeita ao processo de gestão de risco em segurança da informação. Em termos de estimativa de risco, o método procura estimar o impacto do risco numa escala qualitativa e a partir daí definir as medidas de prevenção.

2.5.2 FAIR – Factor Analysis of Information Risk

A *framework* FAIR (Factor Analysis of Information Risk) oferece também uma abordagem baseada numa avaliação qualitativa, numa escala "de muito alto a muito baixo", de vários factores de risco. A *framework*, para além desta escala de medição, inclui também uma taxonomia e nomenclatura padrão para informação de risco, estabelece critérios para a recolha de informação sobre o risco, uma ferramenta computacional para calcular risco e um modelo para analisar cenários de risco complexos [6]. A Figura 8 mostra a decomposição de risco em factores. A recolha de informação sobre estes factores permitirá o cálculo do nível de risco de um sistema de informação.

Figura 8 - FAIR – taxonomia da decomposição de risco

2.5.3 Microsoft Security Risk Management

A Microsoft apresenta também uma abordagem para o processo de gestão de risco - Microsoft Security Risk Management [14] - que em tudo parece estar alinhada com o disposto na norma ISO 31000, definindo-o como um processo contínuo e composto por quatro fases:

- Apreciação de risco que compreende identificar e prioritizar os riscos para o negócio.
- Tomada de decisão face ao risco. Nesta fase são identificadas e avaliadas soluções de controlo baseadas numa análise de custo-benefício.
- Implementação de medidas de controlo para reduzir o risco para o negócio.
- Medição da eficácia das medidas tomadas no sentido de avaliar se estas conferem na realidade o grau de protecção esperado.

A abordagem da Microsoft defende a comunicação como princípio básico ao processo de gestão de risco, sendo o uso de uma linguagem universal condição essencial para o seu sucesso. A Figura 9 apresenta os componentes de risco, considerados essenciais para uma "declaração de risco bem formada".

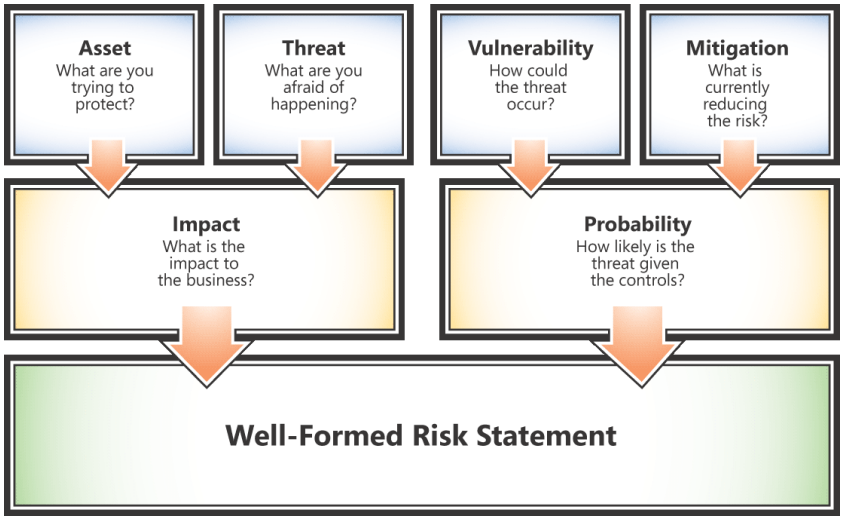

Figura 9 – Microsoft Security Risk Management – componentes do risco [14]

2.6 Abordagens para avaliação do impacto das quebras de serviço

Nesta secção apresentam-se alguns trabalhos relacionados com o tema que esta dissertação pretende tratar em concreto e que de alguma forma acabaram por inspirar o desenvolvimento desta dissertação e simultaneamente reforçar a necessidade de abordagens quantitativas de análise de risco.

Estimar o impacto de incidentes de quebras de serviço, sejam estes gerados por quebras de segurança ou não, é uma tarefa árdua e os métodos já existentes têm falta de base empírica ou não são suficientemente rigorosos, genéricos ou flexíveis. Até então, também não houve nenhum modelo consistente que servisse para a investigação teórica e empírica ou também para a prática profissional.

A *framework* proposta por Thomas et al. [15] adopta um quadro de decisão *ex ante* coerente com a tomada de decisão racional do ponto de vista económico, bem como, mede as consequências das falhas tendo em conta os custos previstos de recuperação, não só da entidade atacada como também de todas as partes interessadas, o que permite uma avaliação mais actualizada do que as teorias tradicionais baseadas no valor dos bens. Esta abordagem inspirou a forma de cálculo dos custos de reputação sugerida pelo presente trabalho.

O modelo proposto é uma árvore de eventos cuja estrutura e condições de ramificação podem ser estimadas, utilizando inferência probabilística a partir de evidências indicadoras de impacto. Esta abordagem pode facilitar a estimativa fiável do modelo quando a evidência é imperfeita, incompleta, intangível, ambígua ou contraditória.

O método proposto pode também ser útil para modelar as consequências do incidente que vão além da organização atacada, incluindo consequências que possam ocorrer em cascata em infra-estruturas críticas.

Apesar dos potenciais benefícios do trabalho, verifica-se que os pressupostos da ideia base ainda carecem de validação, encontrando-se o trabalho numa fase embrionária da investigação e por isso sem resultados práticos para apresentação.

Para além de ser importante relacionar custos com uma falha específica, de forma a possibilitar, por exemplo, a um administrador lutar na justiça pela restituição do valor da sua perda em consequência de uma quebra de um serviço fornecido por terceiros, é ainda mais importante poder tomar medidas efectivas de segurança para evitar ou mitigar os impactos do risco. Sendo por um lado extremamente difícil cobrir todo um sistema em termos de segurança e por outro financeiramente desejável que as medidas se ajustem às possíveis quebras, é imprescindível quantificar o risco para poder quantificar a efectividade das medidas de segurança. Neste sentido, Pieters et al. [16] propõe uma abordagem baseada em modelação que visa garantir a efectividade das medidas de segurança tomadas, discutindo também o conceito de segurança em oposição ao de salvaguarda. Reforça a ideia da necessidade de quantificar aspectos do risco como o esforço do atacante de forma a permitir comparações deste com o potencial impacto do ataque e com o aumento do esforço do atacante que determinada medida de mitigação de risco pode significar.

A *framework* "CAPRA" [17], apresentada por Ayyub et al., pretende ser uma ferramenta de análise quantitativa de qualquer tipo de risco sobre bens ou portefólio. Seguindo um desenvolvimento dos detalhes quantitativos subjacentes a cada fase, foi obtida uma fórmula genérica para qualquer tipo de risco que se assemelha ao modelo de risco de segurança tradicional, onde o risco é o produto de consequência, vulnerabilidade e ameaça, embora com significados claros atribuídos a cada parâmetro. Além disso, fornece também uma técnica simples para capturar as consequências resultantes das interdependências de um portefólio. Os detalhes de como realizar a avaliação são dependentes do tipo de activo, características do portefólio e tipos de risco, e podem variar de acordo com o tempo e necessidades do decisor e também com os recursos analíticos disponíveis. Os requisitos de dados para a CAPRA incluem tanto informação histórica como opiniões de especialistas e a incerteza é tratada conforme cada caso, utilizando técnicas convencionais de propagação e de representação. Um trabalho recente pode sugerir dados de avaliações de risco e vulnerabilidades anteriores, avaliações de instalações semelhantes e opiniões de especialistas para a construção de distribuições dos parâmetros. Estes podem ser agregados utilizando técnicas baseadas em teoria da evidência [18][19].

2.7 Impacto das falhas na confiança dos clientes

A pesquisa por trabalho relacionado foi feita também no sentido de encontrar trabalhos sobre a confiança das pessoas nos serviços bancários e a reputação destes, uma vez que esta foi a área usada na prova de conceito para este trabalho e considero fundamental para lidar com o problema de alguns custos intangíveis do sector bancário.

O papel da confiança acompanha as interacções entre a banca de retalho e o seu cliente em várias dimensões dos meios electrónicos de pagamento. A confiança depende especialmente das relações que se estabelecem tendo por base plataformas tecnológicas. Mukherjee et al. [20] para além de demonstrar que as relações estabelecidas *online* têm maior importância na banca do que nos restantes sectores empresariais, apresenta também o resultado de um estudo efectuado com utilizadores deste tipo de serviço, descrevendo a reputação e a segurança como as duas dimensões da confiança e apontando os principais motivos que estão na origem da criação de um sentimento de confiança que por sua vez gera fidelização entre o cliente e o seu banco.

O grau de dependência que um utilizador vai criando dos serviços que o seu banco disponibiliza através de canais não presenciais, como por exemplo, os meios electrónicos de pagamento ou a banca *online*, faz variar na razão directa o risco de descrédito de um utilizador que se veja subitamente privado de utilizar o serviço. O artigo de Zhengwei Ma [21] fala da valorização que um utilizador atribui a um serviço e

propõe um modelo para analisar empiricamente a ligação entre disponibilidade, fiabilidade e satisfação do cliente.

O trabalho de Lee [22] tem como objectivo desenvolver um modelo de aceitação tecnológica (TAM), enriquecido com um modelo teórico do comportamento planeado (TPB), para prever e explicar as intenções comportamentais dos clientes no que diz respeito à adopção de serviços de banca *online*. O modelo proposto incorpora cinco categorias de percepção do risco para fornecer uma investigação abrangente, cobrindo tanto os aspectos positivos como negativos da banca *online*. Os resultados mostram que o modelo proposto tem um bom poder explicativo e confirma a sua robustez em prever as intenções dos clientes para usar tais serviços. Este método permite também tirar conclusões no sentido de que a utilidade e o benefício associados a este tipo de canal percepcionados pelos clientes, os levam a aceitar o risco. Isto por si só é um indicador que revela que a interrupção do serviço seria um grande motivo de desagrado do cliente podendo levar à ruptura da sua ligação com o banco.

Entendendo as falhas como podendo ser totais ou parciais, considero também importante auferir informação sobre quais as funcionalidades mais valorizadas pelos clientes dos serviços *online*. É exemplo desse tipo de estudo, o trabalho apresentado por Singhal and Padhmanabhan [23]. Este trabalho conclui que o serviço de banca *online* é cada vez mais o serviço bancário mais valorizado pelos clientes, estando a passar do estado de *"nice to have"* para o de *"need to have".* Os principais factores responsáveis por isso são a utilidade dos tipos de transacção oferecidos pelo serviço, a fiabilidade e a segurança.

2.8 Workflow & QoS

A forma mais imediata de medir a fiabilidade dos sistemas desenhados para fornecer muito alta disponibilidade e serem executados continuamente será sem dúvida a probabilidade do sistema não parar durante o intervalo de tempo especificado [24]. O sistema que foi alvo de análise neste trabalho – Multibanco – insere-se nesta categoria, sendo esperado um regime de execução em 24x7 realizando operações em tempo-real.

Cardoso [25] define fiabilidade de uma tarefa como a probabilidade de determinada componente trabalhar de acordo com o esperado pelo seu utilizador seguindo um modelo discreto de tempo, ou seja, *fiabilidade = nº de execuções falhadas ÷ nº de execuções*. O autor propõe um modelo preditivo de QoS (*Quality of Service*) para *workflows* e *webservices* que, baseado nos atributos de QoS de cada tarefa, consegue estimar a QoS para um *workflow* inteiro. São usadas as dimensões tempo, custo, fiabilidade e fidelidade, no entanto, formular genericamente os dois últimos pode não

ser possível e por isso requerer métodos específicos de cada tarefa e de cada tipo de sistema.

Para computar a QoS de um *workflow*, o autor desenvolveu um método de redução estocástico. O método consiste em aplicar iterativamente um conjunto de regras de redução ao *workflow* até que este se reduza a uma única tarefa. Cada vez que uma regra é aplicada, a estrutura do *workflow* vai sofrendo alterações simplificativas. A última e única tarefa restante irá conter as métricas de QoS inerentes ao *workflow* como um todo. As métricas são o tempo do *workflow* em várias vertentes - tempo de resposta, tempo de atraso, tempo mínimo de resposta e tempo de resposta eficiente; o custo do *workflow*; a fiabilidade e a fidelidade deste.

A notação BPMN (Business Process Model and Notation) tem vindo a ser cada vez mais utilizada pelas organizações para modelar os seus processos de negócio, revelando assim esta ferramenta como um meio adequado para analisar e optimizar processos, facto talvez ligado à sua riqueza semântica e facilidade de aprendizagem [26].

Neste contexto surge o trabalho de Respício and Domingos [27] que se propõe a computar a fiabilidade de processos BPMN aplicando o método de redução estocástico de Cardoso [25]. Para tal também perspectiva estender a notação BPMN com informação sobre fiabilidade. Algumas destas regras foram utilizadas na aplicação resultante do presente trabalho para permitir a computação da probabilidade de falha e valor do risco dos sistemas nela analisados, nomeadamente, a regra de redução de blocos sequenciais e a regra de redução de blocos condicionais. Por se tratar de um protótipo, apenas foram utilizadas as regras mais comuns, no entanto, a aplicação irá evoluir no sentido de se alargar o leque de regras usadas de forma a poder acolher maior variedade de sistemas.

2.9 Importância dos SLA

Ao longo dos últimos anos as organizações foram-se tornando cada vez mais dependentes de inúmeros tipos de serviços de tecnologias de informação (TI). A integração de serviços de TI numa organização arrasta consigo a necessidade de operação e exploração desses serviços o que constitui um factor altamente determinante do desempenho dessa organização. Muitas vezes, por questões de gestão estratégica ou falta de *know-how,* esses serviços são prestados por terceiros, o que aumenta ainda mais a importância da sua monitorização e controlo. A exploração e operação de serviços de TI é genericamente designada por "Gestão de serviço" e compreende actividades como monitorização de performance e disponibilidade, suporte, formação e operação técnica. Um dos principais conceitos de gestão de serviço é o SLA (Service Level Agreement) e

o seu objectivo principal é constituir uma ferramenta que permita gerir a expectativa do cliente [28].

Para gerir um serviço de TI de forma adequada, é necessário que haja um consenso sobre o serviço entre o fornecedor e o cliente. Nesta negociação é necessário que ambos os intervenientes fiquem cientes de uma única definição do serviço e de toda a concepção e implementação dos processos do serviço, de forma que possam ser definidos SLA's que na prática não possam ter efeitos nefastos para o cliente em particular [29]. Alguns dos problemas mais comuns existentes nos SLA são:

- **Orientação ao esforço do fornecedor ao invés de resultado do serviço**. Os SLA frequentemente apresentam, por exemplo, tempo de recuperação de um sistema em vez de garantir o tempo de actividade ininterrupta deste.
- **Especificações de serviço pouco precisas.** Algumas especificações, como por exemplo, acerca de disponibilidade referem 98% de disponibilidade. Isto pode significar algo inaceitável como uma semana inteira de indisponibilidade ao longo de um ano (caso 98% signifique 51 semanas).
- **Especificações de serviço incompletas**. Alguns serviços de TI são difíceis de definir como por exemplo "prevenção de catástrofe". Não existe uma boa definição de desastre pois esta só é possível fazer depois de acontecer.
- **Gestão de custos insuficiente**. É difícil por vezes quantificar o custo de um serviço. Este pode envolver variáveis complexas e pode ainda estar relacionado com custos intangíveis.
- **Documentos imperceptíveis**. Os documentos que dão suporte aos SLA apenas conseguem ser interpretados por um grupo restrito de técnicos o que leva por vezes os gestores a encararem esta definição como um ritual que se cumpre sem sentido.

Pelas razões acima descritas é importante que uma organização conheça bem as exigências dos sistemas que delegou em terceiros e conheça os impactos que as suas falhas podem significar. Só assim poderão definir SLA's ajustados à sua realidade e não orientados ao esforço do fornecedor ou seguindo uma qualquer tendência do mercado.

Dada a importância dos SLA, foi objectivo da ferramenta produzida neste trabalho fornecer ao utilizador informação sobre a evolução temporal do impacto das quebras de serviço de modo a auxiliar na especificação de SLA's para fornecedores.

Capítulo 3

Metodologia para quantificação de risco no sistema Multibanco

Neste capítulo apresenta-se a metodologia de quantificação e valoração de risco proposta por este trabalho, aplicada ao sistema Multibanco em particular. Assim começa-se por descrever este sistema, apresentando o seu enquadramento funcional, explicando o funcionamento do protocolo de tempo-real da SIBS e apresentando as possíveis falhas do sistema. De seguida é apresentada a metodologia proposta neste trabalho, descrevendo os princípios em que está assente e o seu posicionamento no processo de gestão de risco. Por fim, apresenta-se a modelação do sistema multibanco na vertente de tempo-real aplicando a referida metodologia.

3.1 Descrição do sistema Multibanco

3.1.1 Descrição funcional

(Conteúdo de natureza confidencial removido)

3.1.2 Protocolo de tempo-real SIBS

(Conteúdo de natureza confidencial removido)

3.1.3 Possíveis falhas

(Conteúdo de natureza confidencial removido)

3.2 Metodologia de quantificação e valoração de risco

(Conteúdo de natureza confidencial removido)

3.3 Modelação do sistema Multibanco (Tempo-real)

(Conteúdo de natureza confidencial removido)

Capítulo 4

Quanto – Aplicação de quantificação de risco

Neste capítulo apresenta-se o trabalho de desenvolvimento de um protótipo da aplicação informática que funcionará suportada pela metodologia anteriormente descrita.

Começa-se por apresentar a especificação de requisitos efectuada e que esteve na base do trabalho, a arquitectura da aplicação e respectivos sistemas envolventes, as ferramentas utilizadas e a análise funcional da aplicação.

4.1 Especificação de requisitos

A aplicação "Quanto" pretende ser uma solução para efectuar a quantificação de risco associado a quebras de serviço, através de uma análise que permita obter a valoração de processos de negócio e quantificação do risco associado a estes.

Nesta secção apresentam-se os requisitos que se pretende satisfazer com a aplicação.

4.1.1 Requisitos funcionais

Os requisitos funcionais traduzem as principais características pretendidas para aplicação de maneira que esta possa cumprir os objectivos para que foi implementada. Assim foram definidos os seguintes requisitos:

- **Caracterização de sistemas**. Permitir a descrição de sistemas e a sua decomposição em processos.
- **Caracterização de processos**. Permitir a descrição de processos, estabelecer relação entre eles e sua associação a sistemas.
- **Registo de activos**. Permitir o registo de activos associados aos processos, definir o seu valor e actualização periódica (valorização ou desvalorização). Este registo tem como objectivo poder valorar os processos.

- **Registo de variáveis**. Para além de permitir valorar processos através dos activos que lhes estão associados, é necessário conseguir contabilizar outros valores variáveis que possam estar associados aos processos ou ser gerados por estes.
- **Registo de ameaças e vulnerabilidades**. As ameaças a que o sistema está sujeito devem ser registadas e associadas aos respectivos processos com a respectiva probabilidade de ocorrência e percentagem de mitigação.
- **Simulação de falhas**. A aplicação deve permitir simular uma falha em determinado processo pela concretização de uma determinada ameaça e permitir a sua análise em termos do potencial impacto que o sistema sofreria.
- **Análise de falhas**. A aplicação deve possibilitar efectuar o registo de uma falha real ocorrida no sistema, permitindo apurar qual foi o seu impacto no sistema e portanto a eventual perda gerada.

4.1.2 Requisitos não funcionais

Para além das características que permitem que a aplicação cumpra as suas funções essenciais, esta tem de possuir também algumas características acessórias mas que constituem contribuições necessárias para poder corresponder aos seus objectivos em pleno.

Assim, foram definidos os seguintes requisitos não funcionais:

- **Integração**. De forma a permitir efectuar quer estimativas, quer análises de impacto de falhas é necessário que seja possível integrar na aplicação, de forma fácil, informação oriunda de outros sistemas.
- **Usabilidade**. Dada a possível complexidade dos sistemas que podem ser objecto de análise é necessário que a aplicação funcione de forma simples e intuitiva e contenha mecanismos que permitam acelerar a caracterização de processos assim como a extracção de estimativas e análises de impacto.

4.2 Arquitectura

(Conteúdo de natureza confidencial removido)

4.3 Ferramentas utilizadas

As ferramentas escolhidas para o desenvolvimento da aplicação tiveram em linha de conta o facto de se poder tirar partido das licenças de desenvolvimento que a instituição já possui, o facto de se pretender um ambiente de desenvolvimento rápido e a

obtenção de uma aplicação *desktop* Windows que é o sistema operativo mais usado pelos utilizadores a que esta se destina. Assim a escolha recaiu sobre a *framework* .net e o Microsoft Visual Studio Professional 2013.

Em termos de base de dados, foi escolhido o MySQL 5.6 que para além de se tratar de um produto *freeware,* fornece uma interface de utilizador bastante completa, intuitiva e facilitadora da importação de dados de outros sistemas.

4.4 Funcionalidades

(Conteúdo de natureza confidencial removido)

4.4.1 Registo de Sistema

(Conteúdo de natureza confidencial removido)

4.4.2 Registo de Processo

(Conteúdo de natureza confidencial removido)

4.4.3 Registo de Activo

(Conteúdo de natureza confidencial removido)

4.4.4 Registo de Variável

(Conteúdo de natureza confidencial removido)

4.4.5 Registo de Ameaça

(Conteúdo de natureza confidencial removido)

4.4.6 Associação de Processos e Sistemas

(Conteúdo de natureza confidencial removido)

4.4.7 Diagrama do sistema

(Conteúdo de natureza confidencial removido)

4.4.8 Associação de Processos e Activos

(Conteúdo de natureza confidencial removido)

4.4.9 Associação de Processos e Variáveis

(Conteúdo de natureza confidencial removido)

4.4.10 Associação de Processos e Ameaças

(Conteúdo de natureza confidencial removido)

4.4.11 Registo de Mitigação de risco

(Conteúdo de natureza confidencial removido)

4.4.12 Simulação de Falha

(Conteúdo de natureza confidencial removido)

4.4.13 Análise de falha

(Conteúdo de natureza confidencial removido)

4.4.14 Importação de dados

(Conteúdo de natureza confidencial removido)

4.4.15 Funções de administração

(Conteúdo de natureza confidencial removido)

Capítulo 5

Avaliação da Ferramenta Quanto

Neste capítulo apresentam-se todas as avaliações que se conseguiram efectuar para o trabalho desenvolvido, envolvendo os futuros utilizadores da aplicação. Apresentam-se também as principais conclusões retiradas acerca da utilização da ferramenta e da forma como esta responde às necessidades dos utilizadores a que se destina.

5.1 Avaliação

Para recolher a opinião dos utilizadores a quem se destina a aplicação, foi realizada uma apresentação desta, acompanhada de discussão da metodologia que lhe está associada com base em revisão da literatura efectuada. Seguidamente a aplicação foi entregue para utilização exploratória.

Na aplicação foram introduzidos os dados relativos ao sistema Multibanco - vertente receptora, conforme descrito na secção 3.3. Posteriormente, através de ficheiros "csv", foram extraídos do sistema em análise e importados para a aplicação dados relativos ao valor e frequência de cada variável e activo configurados nesta de forma a permitir efectuar estimativas de risco através de simulações de falha, bem como, análises de falha tendo por base informação de histórico do sistema analisado. Os valores apresentados e extraídos da aplicação são fictícios.

A recolha de informação dos principais utilizadores acerca da usabilidade e utilidade da aplicação foi baseada num questionário SUS (System Usability Scale) [30] e num questionário desenhado para classificar a aplicação numa escala de utilidade, respectivamente.

5.1.1 Simulação de falha

Esta funcionalidade foi usada, conforme descrito no subcapítulo 4.4 – Funcionalidades na secção 4.4.12 – Simulação de Falha, para estimar o risco de uma

quebra de serviço, tendo por base informação de histórico acerca do comportamento do sistema em determinado período considerado como tipicamente normal.

(Conteúdo de natureza confidencial removido)

5.1.2 Alteração de configuração do sistema

Uma das utilidades que se pretende dar a esta ferramenta é a de poder observar alterações no valor do risco estimado decorrentes de alterações que se possam efectuar na configuração dos sistemas analisados. Por exemplo, no caso do sistema Multibanco surge muitas vezes a dúvida se devemos ou não configurar determinada operação como "RTOnly" de forma a diminuir as hipóteses de fraude e consequente descoberto não autorizado.

Apresenta-se aqui uma experiência exemplificativa, utilizando as mesmas parametrizações que foram utilizadas na simulação apresentada na secção 5.1.1.

(Conteúdo de natureza confidencial removido)

5.1.3 Análise de falha

Esta funcionalidade foi usada, conforme descrito no subcapítulo 4.4 – Análise Funcional na secção 4.4.13 – Análise de Falha, para analisar o impacto de uma falha do sistema, tendo por base informação de histórico acerca do comportamento do sistema em determinado período registado no passado como tendo ocorrido falha no sistema.

(Conteúdo de natureza confidencial removido)

5.2 Resultados gerais da avaliação

Nesta secção apresentam-se os resultados da avaliação a que a ferramenta resultante deste trabalho foi submetida, para cada uma das suas contribuições. As impressões recolhidas da apresentação e utilização da ferramenta assim como da discussão da metodologia associada, foram cruzadas com a informação registada através dos questionários efectuados aos utilizadores acerca da usabilidade e utilidade da ferramenta.

De uma forma geral conclui-se que a ferramenta satisfaz todos os requisitos a que se propôs e os utilizadores concordam que ela oferece os contributos previstos no início e descritos na secção 1.3, fazendo no entanto algumas ressalvas.

Metodologia de quantificação e valoração de risco

Após uma breve revisão da principal literatura que serviu de base a esse trabalho, nomeadamente as normas ISO relacionadas com o processo de gestão de risco, foi apresentada e discutida a metodologia sugerida por este trabalho. Tendo em conta a complexidade do sistema Multibanco, sistema sobre o qual se pretende aplicar o processo de análise de risco de uma forma quantitativa em vez de qualitativa, a opinião dos utilizadores foi unânime em aceitar a metodologia de quantificação de risco proposta como adequada para dar resposta a esta necessidade.

Foi realçado o facto de esta metodologia estar construída de forma simples, baseada nas cinco componentes – Processo, activos, valores variáveis, ameaças e falhas, o que permitirá a sua aplicação a outros sistemas.

Captar os custos intangíveis como o da reputação é sempre uma tarefa difícil senão impossível. A sugestão de uma abordagem baseada nos custos de recuperação em detrimento das baseadas no valor do activo foi considerada como uma abordagem exequível e que vai ao encontro da filosofia de tomada de decisão actualmente vigente na organização baseada em análise *custo-benefício.*

Estimativa de risco

As duas principais valências da aplicação desenvolvida são por um lado a possibilidade de estimar risco de uma falha futura e por outro quantificar perdas decorrentes de uma quebra de serviço efectivamente ocorrida no passado. Relativamente à primeira foi salientada a importância da possibilidade de importação de informação de histórico do sistema em análise, proporcionando assim previsões mais sustentadas.

Análise do impacto de falhas

Relativamente à segunda valência desta aplicação, a possibilidade de quantificar perdas decorrentes de uma quebra de serviço ocorrida no passado foram feitas ressalvas no sentido de existir necessidade de se aperfeiçoar a identificação dos períodos homólogos, com os quais se fazem comparações de padrões entre estes e o período de falha para apuramento do valor da perda. Existem alguns padrões de utilização da rede multibanco. Por exemplo, ao dia 8 de cada mês existe sempre um volume de transacções superior aos outros dias ou ao domingo existe sempre uma redução do volume de transacções face aos outros dias da semana. Isto faz com que não se possam comparar dias com características diferentes sob pena de sermos induzidos em erro identificando um falso padrão de falha.

O facto da introdução do conceito de "Custos adicionais em caso falha" foi visto como extremamente importante, uma vez que no sistema Multibanco nem sempre a quebra de serviço se traduz numa simples diminuição do valor gerado pelo processo. Por vezes, apenas o aumento deste tipo de custo, que neste caso representa o descoberto não autorizado em que o banco pode incorrer devido à autorização de operações ter sido feita pela SIBS em detrimento do banco, pode representar o valor da perda resultante de uma quebra de serviço.

Representação de sistemas

O funcionamento da aplicação informática produzida está dependente da existência de uma caracterização dos vários processos que compõe um sistema, com informação relevante do ponto de vista da análise de risco. Adicionalmente, o utilizador poderá utilizar esta ferramenta para saber a composição de um determinado sistema podendo inclusive visualizá-lo sobre a forma de um diagrama BPMN. No entanto, para que isto possa acontecer é necessário que o utilizador introduza os dados relativos à composição do seu sistema na aplicação em vez de aproveitar os diagramas BPMN já existentes na organização para importar essa informação. Esta funcionalidade implicaria substituição da aplicação actualmente utilizada para diagramação, por uma que produzisse um diagrama em xml que pudesse ser interpretado pela aplicação Quanto, criando na sua base de dados a estrutura de um determinado sistema.

Outro aspecto que mereceu destaque pela positiva foi o facto de a aplicação indicar quais os processos mais críticos, permitindo assim direccionar a atenção dos responsáveis pelos sistemas para equacionar medidas de mitigação auxiliando simultaneamente na justificação de algum investimento que seja necessário fazer.

Avaliação de diferentes configurações de um sistema

No sistema Multibanco em particular, equaciona-se muitas vezes a hipótese de alterar o funcionamento de determinada transacção de "RTOnly" para não "RTOnly" para evitar a fraude ou diminuir o custo com o descoberto não autorizado. No entanto esse tipo de alteração pode trazer mais custos do que benefícios. Podemos conseguir diminuir o valor a descoberto mas aumentar o risco de reputação por quebra de serviço nessas operações.

Com esta ferramenta os utilizadores conseguem modelar configurações diferentes das transacções no sistema em análise de forma permitir a comparação entre os níveis de risco daí resultantes, possibilitando tomar essas decisões baseadas numa análise *custo-benefício*.

Definição de SLA

Alguns dos equipamentos que suportam o sistema em análise são administrados por terceiros. Apesar de existir um SLA para este sistema, existe a noção de que estes foram definidos de forma subjectiva ou até seguindo aquilo que são os hábitos do mercado para sistemas de natureza distinta. Esta ferramenta pode auxiliar na tarefa de ajuste deste SLA suportando uma decisão de diminuição do tempo de recuperação ou imposição de sanções, uma vez que fornece uma visão da evolução temporal do impacto financeiro das quebras de serviço.

5.3 Avaliação de usabilidade da aplicação Quanto

Após um período de utilização da ferramenta, os utilizadores responderam a um questionário elaborado com o objectivo de aferir o nível de usabilidade da aplicação (SUS) [30]. O questionário encontra-se no Anexo 14 e os resultados finais do questionário sobre a usabilidade da aplicação estão representados na Tabela 3.

Tabela 3 - Resultados obtidos do questionário de usabilidade - SUS

Utilizador	Resultado	Percentil
U1	34	85
U2	29	72,5
U3	33	82,5

Os utilizadores respondem a este questionário utilizando uma escala de 1 a 5, sendo que 1 significa “discordo totalmente” e 5 significa “concordo totalmente”. Para obter o resultado do questionário, ao valor da resposta das perguntas de caracter positivo é subtraído o valor 1. Relativamente às perguntas de caracter negativo o seu valor é subtraído a 5. Desta forma cada pergunta é valorada de zero a quatro e o somatório de todas as respostas reflecte o resultado do questionário num valor entre 0 e 40. Para converter este valor em percentil, ou seja, num valor entre 0 e 100, multiplica-se por 2,5.

O valor médio dos percentis obtido é 80 que na escala do SUS corresponde a um “B”. Conforme se pode visualizar na Figura 10, corresponde à segunda nota mais alta.

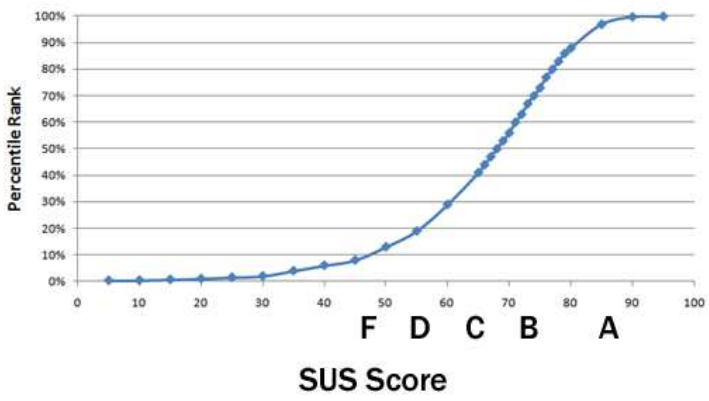

Figura 10 - Curva de scoring de usabilidade SUS [31]

Os principais aspectos positivos de realce deste questionário são o facto de não ser considerado um sistema desnecessariamente complexo, não requer grande aprendizagem e ter uma boa integração de funções.

Como aspecto menos positivo destaca-se o facto de os utilizadores, apesar da pontuação elevada que atribuíram às questões citadas no parágrafo anterior, considerarem que irão necessitar da ajuda de um técnico para conseguirem utilizar o sistema.

5.4 Avaliação de utilidade da aplicação Quanto

Seguindo o formato do questionário SUS, confrontaram-se também os utilizadores com um questionário direccionado para aferir da utilidade da aplicação. O questionário encontra-se no Anexo 15 e os resultados finais do questionário sobre a usabilidade da aplicação estão representados na Tabela 4.

Tabela 4 – Resultados obtidos do questionário de utilidade

Utilizador	Resultado	Percentil
U1	37	92,5
U2	32	80
U3	36	90

O valor médio dos percentis obtido é 87,5 que na escala do SUS já corresponde a um "A". Conforme se pode visualizar na Figura 10, corresponde à nota mais alta.

Todas as questões foram respondidas com notas elevadas mas os principais aspectos positivos de realce deste questionário são o facto de os utilizadores considerarem que esta aplicação permitirá também analisar outros sistemas bancários assim como outros sistemas representáveis por *workflow*. Consideram também que é

importante saber o valor de cada processo e que a aplicação representa um contributo importante para a avaliação do risco no sistema Multibanco.

Capítulo 6

Conclusão

Neste capítulo apresenta-se uma conclusão final sobre todo o trabalho efectuado. Inicia-se por uma revisão crítica dos objectivos da dissertação, passando pela perspectiva de trabalho futuro, terminando com conclusões finais acerca dos fundamentos teóricos e resultados obtidos com este trabalho.

6.1 Revisão de objectivos

O que se pretendia obter com a realização deste trabalho era a definição de uma metodologia que operacionalizasse de forma pragmática uma das componentes do processo de gestão de risco – a análise de risco. Era também objectivo deste trabalho o desenvolvimento de uma aplicação informática que suportada por essa mesma metodologia permitisse concretizar essa actividade. Considera-se terem sido satisfatoriamente alcançados todos os objectivos definidos no seu início.

A metodologia apresentada foi pensada, por um lado, respeitando as definições gerais do processo de gestão de risco ditadas pelo conjunto de normas e melhores práticas existentes para esta matéria e, por outro, tendo em conta a necessidade da instituição e dos utilizadores a que se destina.

No que respeita à aplicação desenvolvida, foi demostrado ao longo deste relatório que se conseguiu uma ferramenta que apesar de se tratar de um protótipo com larga margem de crescimento, regista níveis de usabilidade e utilidade suficientes para se considerar que serve plenamente o propósito para o qual foi desenhada. Os utilizadores responsáveis por analisar e avaliar o risco inerente ao funcionamento dos sistemas podem agora contar com um meio fácil, rápido e sistematizado de obter conhecimento acerca destes.

6.2 Trabalho futuro

A aplicação "Quanto" será um projecto em contínua evolução. Estão já identificadas algumas melhorias que se podem efectuar a curto e médio prazo, para melhorar a sua usabilidade e utilidade. Outras melhorias irão necessariamente surgir, uma vez que não se trata de uma aplicação "chave na mão" mas sim de algo que terá de evoluir em paralelo com desenvolvimentos que possam surgir nos sistemas analisados e também com novas necessidades identificadas pelos utilizadores.

Em termos de usabilidade propõe-se a evolução do módulo de definições para que permita efectuar o *forward engineering* de um sistema representado em BPMN com a ajuda de um qualquer sistema BPMS para a base de dados da aplicação "Quanto". Desta forma simplificar-se-ia a utilização de maneira a permitir utilizar diagramas já existentes do seu sistema para o carregar na base de dados com apenas um *click*. Depois de ter todos os processos e respectivas relações entre eles carregados, o utilizador ficaria apenas com o encargo de completar a restante informação acerca dos processos.

Em termos de melhorias a limitações do processo, propõe-se a introdução de mais regras de redução no cálculo de risco de modo a alargar a capacidade de analisar sistemas com diferentes características. Neste momento a aplicação usa as mais usuais, para blocos sequenciais e blocos condicionais, podendo alargar o leque para as restantes aplicáveis a blocos paralelos, cíclicos, de rede e tolerantes a faltas.

Um refinamento da forma como se identificam os períodos homólogos a um período de falha especificado é uma melhoria apontada pelos utilizadores e deve ser efectuada a breve prazo de forma a permitir análises mais fidedignas.

6.3 Conclusões finais

Apresenta-se nesta secção, uma visão geral e objectiva, sobre três itens fundamentais. Os fundamentos teóricos que estão na base desta dissertação, o trabalho realizado e os resultados obtidos.

Quanto aos fundamentos teóricos do trabalho, não obstante o facto desta área de estudo se tratar de uma área cuja discussão assume cada vez mais importância na actualidade, este trabalho parece sugerir uma abordagem alternativa face ao que já existe. Com o intuito de responder em primeiro lugar à necessidade que uma organização tem de monitorizar os seus sistemas, em particular o Multibanco, não deixa de ter a simplicidade e flexibilidade suficientes para torna-la aplicável a outros sistemas.

Os fundamentos teóricos apontados no início deste trabalho assentavam na necessidade de existência de um meio sistematizado e fiável para efectuar a apreciação

de risco. Tem sido cada vez mais usual que a estratégia das organizações passe pela terciarização de serviços. Isto implica muitas vezes ter os sistemas informáticos que suportam o seu negócio, fora de portas, diminuindo assim o controlo que teriam sobre estes, aumentando os factores de risco e as necessidades de monitorização, imputação de responsabilidades e aplicação de SLA's. É prática da gestão de topo definir os objectivos a atingir pela sua organização, efectuando simultaneamente o levantamento de riscos inerentes ao percurso que é necessário efectuar para os atingir, bem como, formas de controlar esses mesmos riscos dentro dos limites de aceitação de risco definidos pela organização. A eficácia destas formas de controlo, depende grandemente da qualidade de informação obtida no processo de apreciação de risco e em particular da sua componente de análise de risco. Quanto mais informação de histórico do sistema for trabalhada, menores serão as margens de erro da apreciação de risco.

O trabalho efectuado propõe um meio de obter conhecimento profundo acerca de um sistema que permita efectuar uma avaliação de risco mais informada, com base em estimativas mais fiáveis, o que permitirá sustentar as decisões sobre as formas de controlo e tratamento do risco. É neste contexto que foram definidos os objectivos e requisitos da aplicação produzida e cujos resultados experimentais parecem confirmar a sua validade.

Foi conseguida uma aplicação que permite recolher informação acerca dos processos que compõem um sistema, incluindo os activos que lhes estão associados e todas as variáveis capazes de influenciar o seu valor. Com esta informação a ferramenta consegue cumprir duas grandes funções, por um lado, a simulação de falhas que permite fazer um cálculo previsional do impacto das falhas e por outro, a análise de falhas que permite obter um valor aproximado do custo das falhas ocorridas no passado. Simultaneamente permite identificar os processos críticos do sistema de forma permitir direccionar esforços de controlo de risco. Permite ainda obter uma perspectiva da evolução temporal do risco ou impacto de falha o que é útil para o cálculo de SLA's sobre as actividades de recuperação do sistema.

Abreviaturas

- **SIBS**: Sociedade Interbancária de Serviços. Entidade responsável pelo funcionamento da rede interbancária em Portugal e detentora da marca "Multibanco". Está interposta nas comunicações entre todos os bancos em Portugal.
- **RT:** Real Time.
- **CA:** Caixa Automática disponibilizada para efectuar operações bancárias e não bancárias na rede Multibanco.
- **ATM:** Sigla inglesa para caixa automática.
- **TPA:** Terminal de Pagamento de serviços. Terminal instalado junto de um comerciante para que este possa efectuar pagamento de compras ou serviços.
- **PTR:** Plano de tratamento de risco.
- **SOA:** Statement of applicability. Declaração de aplicabilidade usada no âmbito do processo de tratamento de risco.
- **SLA:** Service level agreement. Acordo de nível de serviço. Estabelece métricas a respeitar no fornecimento de um serviço. Por exemplo "tempo de recuperação de um sistema não superior a quatro horas".
- **SUS:** System Usability Scale. Escala de usabilidade do sistema. Pontuação obtida através de um inquérito feito aos utilizadores que classifica a aplicação em determinado percentil de usabilidade.
- **SLE**: Single loss expectancy. Refere-se ao valor de perda esperado para uma falha.
- **ARO**: Annualized risk occurrence. Refere-se ao número de ocorrências esperadas no período de um ano.
- **ALE**: Annualized loss expectancy. Refere-se ao valor da perda anual esperada. ALE = SLE x ARO

Glossário

- **Cliente:** cliente final que utiliza serviços bancários.
- **Utilizador de balcão**: utilizador que pertence à organização e efectua atendimento ao público.
- **Multibanco**: Termos que genericamente representa o sistema interbancário português, agregando a própria marca Multibanco e várias outras marcas internacionais como a VISA, Mastercard, Amex entre outras. Representa não só a emissão de cartões bancários como também a disponibilização de serviços em terminais.
- **Sistema RT**: sistema composto pelos servidores, redes de dados e comunicações que executam um protocolo de Tempo-real entre a instituição bancária e a SIBS. Este servidor processa mensagens na vertente receptora e emissora.
- **Mensagens de vertente receptora:** são aquelas originadas na SIBS (ex: levantamento de dinheiro em CA ou Compra em TPA), atingem o servidor RT e são reencaminhadas para o servidor central do qual obtém a resposta para envio à SIBS.
- **Mensagens de vertente emissora**: são aquelas que são originadas na instituição bancária e são enviadas à SIBS com o intuito de realizar uma operação no sistema interbancário. Este tipo de operações poderá ter origem no próprio sistema central, ou nos canais não presenciais como a banca online, mobile ou rede privada de ATM's.
- **Sistema Central**: sistema onde corre a aplicação bancária *"core"* do banco.
- **Canais não Presenciais**: por oposição aos canais que funcionam assistidos por um utilizador pertencente à organização, designam-se por canais não presenciais aqueles que permitem que o cliente final interaja com o sistema central de forma autónoma. São exemplos a banca online, mobile e a rede própria de ATM's.

Bibliografia

[1] Ionita, D. (2013). Current established risk assessment methodologies and tools.

[2] Tan, D. (2002). Quantitative Risk Analysis Step-By-Step. *SANS Institute. Retrieved July*, *23*, 2011.

[3] Jorge, N. D. S. (2010). Reputação: um elemento diferenciador e protector face a crises organizacionais.

[4] NP ISO 31000:2013 (2013). Gestão do risco – princípios e linhas de orientação. Norma Portuguesa.

[5] ISO / IEC TR 13335-1 (2004). Information technology- Security techniques-management of information and communications technology security. Part 1: Concepts and models for information and communication technology security management.

[6] Whitman, M., & Mattord, H. (2010). *Management of Information Security*. Cengage Learning.

[7] ENISA, Technical Department of ENISA Section Risk Management. (2012). Introduction to Return on Security Investment. ENISA

[8] ENISA, Technical Department of ENISA Section Risk Management. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report, ENISA.

[9] Rausand, M. (2013). *Risk assessment: Theory, methods, and applications* (Vol. 115). John Wiley & Sons.

[10] ISO/IEC 27000. (2008). Information technology Security techniques - information security management systems - Overview and vocabulary.

[11] ISO/IEC 27005. (2008). Information technology Security techniques - information security management

[12] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*.

[13] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process* (No. CMU/SEI-2007-TR-012). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

[14] Microsoft. (2006). Microsoft Security Risk Management Guide.

[15] Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. (2013, June). How Bad Is It?–A Branching Activity Model to Estimate the Impact of Information Security Breaches. In *Paper submitted to the 12th Workshop on the Economics of Information Security. Accessed* (Vol. 30).

[16] Pieters, W., Probst, C. W., Lukszo, S., & Montoya, L. (2014). Cost-effectiveness of Security Measures: A model-based Framework. *Approaches and Processes for Managing the Economics of Information Systems*, 139.

[17] Ayyub, B. M., McGill, W. L., & Kaminskiy, M. (2007). Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework. *Risk analysis*, *27*(4), 789-801.

[18] Zadeh, L. A. (1986). A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination. AI magazine, 7(2), 85.

[19] Guan, J. W., & Bell, D. A. (1992). Evidence Theory and Its Applications.

[20] Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, *21*(1), 5-15.

[21] Ma, Z. (2012). Assessing serviceability and reliability to affect customer satisfaction of internet banking. *Journal of Software*, *7*(7), 1601-1608.

[22] Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130-141.

[23] Singhal, D., & Padhmanabhan, V. (2008). A study on customer perception towards internet banking: Identifying major contributing factors. *Journal of Nepalese business studies*, *5*(1), 101-111.

[24] Koren I, Krishna CM. (2007). Fault tolerant systems. Morgan Kaufmann.

[25] Cardoso AJS. (2002). Quality of service and semantic composition of workflows (Doctoral dissertation, University of Georgia).

[26] OMG, B. P. M. (2011). Notation (BPMN) Version 2.0 (2011). *Available on: http://www. omg. org/spec/BPMN/2.0*.

[27] Respício, A., & Domingos, D. (2015). Reliability of BPMN Business Processes. *Procedia Computer Science*, *64*, 643-650.

[28] itSMF UK (2012). An introductory overview of ITIL v3. The Stationery Office.

[29] Bouman, J., Trienekens, J., & Van der Zwan, M. (1999). Specification of service level agreements, clarifying concepts on the basis of practical research. In *Software Technology and Engineering Practice, 1999. STEP'99. Proceedings* (pp. 169-178). IEEE.

[30] Brooke, J. (1996). SUS-A quick and dirty usability scale. *Usability evaluation in industry*, *189*(194), 4-7.

[31] Jeff Sauro (2011). Measuring usability with the system usability scale (sus). http://www.measuringusability.com/sus.php.

Anexos

Anexo 1 – Registo de Sistema

(Conteúdo de natureza confidencial removido)

Anexo 2 – Registo de Processo

(Conteúdo de natureza confidencial removido)

Anexo 3 – Registo de Activo

(Conteúdo de natureza confidencial removido)

Anexo 4 – Registo de Variável

(Conteúdo de natureza confidencial removido)

Anexo 5 – Registo de Ameaça

(Conteúdo de natureza confidencial removido)

Anexo 6 – Associação de Processos e Sistemas

(Conteúdo de natureza confidencial removido)

Anexo 7 – Diagrama do Sistema

(Conteúdo de natureza confidencial removido)

Anexo 8 – Associação de Processos e Activos

(Conteúdo de natureza confidencial removido)

Anexo 9 – Associação de Processos e Variáveis

(Conteúdo de natureza confidencial removido)

Anexo 10 – Associação de Processos e Ameaças

(Conteúdo de natureza confidencial removido)

Anexo 11 – Registo de Mitigação de Risco

(Conteúdo de natureza confidencial removido)

Anexo 12 – Simulação de falha

(Conteúdo de natureza confidencial removido)

Anexo 13 – Análise de falha

(Conteúdo de natureza confidencial removido)

Anexo 14 – Questionário sobre usabilidade - SUS

Pergunta	U1	U2	U3
1. Acho que vou gostar de usar este sistema frequentemente	3	2	2
2. Considero este Sistema desnecessariamente complexo	4	4	4
3. Achei o Sistema fácil de usar	3	2	3
4. Acho que vou precisar da ajuda de um técnico para conseguir usar este sistema	2	1	3
5. Considero que as várias funções deste sistema estão bem integradas	3	4	3
6. Acho que há muita inconsistência no sistema	4	3	4
7. Acho que a maioria das pessoas aprenderá a usar este sistema rapidamente	4	3	3
8. Acho o sistema muito complicado de usar	4	3	4
9. Sinto-me confiante a usar este sistema	3	3	3
10. Precisei de aprender um conjunto grande de coisas antes de estar preparado para usar este sistema	4	4	4
Pontuação	34	29	33
Percentil	85	72,5	82,5

Anexo 15 – Questionário sobre utilidade

Pergunta	U1	U2	U3
1. Esta aplicação representa um contributo importante para a avaliação do impacto de falhas no sistema de multibanco	3	3	3
2. Dificilmente se conseguirá que esta aplicação se adapte para analisar outro sistema bancário	4	4	4
3. Esta ferramenta representa um contributo importante para a avaliação do risco do sistema de multibanco	4	4	4
4. Acho importante o facto da aplicação permitir saber o valor de cada processo	4	4	4
5. Esta ferramenta representa um contributo importante para a tomada de decisão relativamente aos pontos críticos no sistema de multibanco	4	3	4
6. Esta ferramenta não me ajuda a calcular SLA's para exigir a fornecedores	4	2	4
7. A utilização de variáveis permite representar qualquer factor de valoração dos processos, mesmo que este factor seja dinâmico	3	3	3
8. Consigo imaginar uma adaptação desta ferramenta para outros sistemas representáveis por workflow	4	4	3
9. Esta ferramenta é útil para prever variações de risco decorrente de alterações efectuadas na estrutura do sistema	3	2	3
10. Esta ferramenta não facilita a execução cíclica do processo de gestão de risco	4	3	4
Pontuação	37	32	36
Percentil	92,5	80	90